

A Weakest Pre-Expectation Semantics for Mixed-Sign Expectations

Benjamin Lucien Kaminski^{†‡} and Joost-Pieter Katoen[†]

[†]Software Modeling and Verification Group
RWTH Aachen University, Germany

Email: {benjamin.kaminski,katoen}@cs.rwth-aachen.de

[‡]Currently on leave at the Programming Principles, Logic and Verification Group
University College London, United Kingdom

Abstract—We present a weakest-precondition-style calculus for reasoning about the expected values (pre-expectations) of *mixed-sign unbounded* random variables after execution of a probabilistic program. The semantics of a while-loop is defined as the limit of iteratively applying a functional to a zero-element just as in the traditional weakest pre-expectation calculus, even though a standard least fixed point argument is not applicable in our semantics. A striking feature of our semantics is that it is always well-defined, even if the expected values do not exist. We show that the calculus is sound and allows for compositional reasoning. Furthermore, we present an invariant-based approach for reasoning about pre-expectations of loops.

I. INTRODUCTION

Probabilistic programs are programs that support choices like “execute program C_1 with probability $1/3$ and program C_2 with probability $2/3$ ”. Describing randomized algorithms has been the classical application of probabilistic programs. Applications in biology, machine learning, quantum computing, security, and so on, have recently led to a rapidly growing interest in such programs [1]. Although probabilistic programs syntactically are normal-looking programs, reasoning about their correctness is intricate. The key property of program termination exemplifies this. Whereas a classical program terminates or not, this is no longer true for probabilistic programs. They can diverge, but this may happen with probability 0. In addition, in contrast to classical programs that either do not terminate at all or terminate in finitely many steps, a probabilistic program may take infinitely many steps on average to terminate, even if its termination probability is 1.

Establishing correctness of probabilistic programs needs—even more so than ordinary programs—formal reasoning. Weakest-precondition (wp) calculi à la Dijkstra [2] provide an important tool to enable formal reasoning. To develop such calculi for probabilistic programs, one has to take into account that due to its random nature, the final state of a program on termination need not be unique. Thus, rather than a mapping from inputs to outputs (as in Dijkstra’s approach), probabilistic programs can be thought of mapping an initial state to a *distribution* over possible final states. More precisely, we may obtain *sub*-distributions where the “missing” probability mass

represents the likelihood of divergence. Given a random variable f (e.g. $f = x^2 + y$, where x and y are program variables) and an initial state σ , a key issue is to determine f ’s expected value¹ on the probabilistic program’s termination. This was first studied in Kozen’s seminal work on probabilistic propositional dynamic logic (PPDL) [4]. Its box- and diamond-modalities provide probabilistic versions of Dijkstra’s weakest (liberal) preconditions. Amongst others, Jones [5], Hehner [6], and McIver & Morgan [3] have furthered this line of research, e.g. by considering non-determinism and proof rules for loops. Recently, Kaminski *et al.* [7] provided wp-style reasoning about the expected run-time of probabilistic programs while Olmedo *et al.* [8] consider recursion.

All these works (except PPDL) make an important—though restrictive—assumption: the random variable f maps program states to the *non-negative* reals. In McIver & Morgan’s terminology, such random variables f are called *expectations*. That is to say, the aforementioned approaches do not deal with *mixed-sign* expectations, i.e. expectations that can be negative, or even negative and positive. McIver & Morgan [3, pp. 70] forbid mixed-sign expectations altogether and argue that “For mixed-sign or unbounded expectations, however, well-definedness is not assured: such cases must be treated individually. [...] That is, although [a program] itself may be well defined, the greatest pre-expectation [for $f = (-2)^n$] is not—and that is a good reason for avoiding mixed signs in general.” A workaround is to assume bounded negative values [9], but this also provides no general solution.

An exception to the widespread and generally condoned neglect of unbounded mixed-sign expectations is Kozen’s PPDL [4] as it provides an expectation transformer semantics for probabilistic programs with respect to general measurable post-expectations f and thus does *not* forbid mixed-sign expectations altogether. PPDL’s proof rule for *reasoning* about while loops, however, requires f to be non-negative [4, Section 4, page 168: the “while rule”]. This proof rule is hence unfit for reasoning about mixed-sign expectations. In fact, three out of four rules of the deduction system of PPDL that deal with iteration (and therefore with loops) require f to be non-negative and are hence not

This work was supported by the Excellence Initiative of the German federal and state government and by the CDZ project CAP (GZ 1023).

¹Commonly called pre-expectation [3].

applicable to reasoning about mixed-sign post-expectations f [4, Section 4: Rules (8), (9), and the “while rule”]. The only exception to this is a rule that allows for upper bounding the *pre-expectation* by a *non-negative function*, even if f is mixed-sign [4, Section 4: Rule (10)]. This rule, however, is insufficient for upper-bounding the pre-expectation by a negative value, which in practice can be desirable and is possible in our calculus, see Example 4.

Another drawback of PPDL is that reasoning even about simple programs and properties can become quite involved, requiring a fairly high degree of mathematical reasoning, i.e. to say that PPDL requires a lot of reasoning inside the program semantics while the approach of McIver & Morgan and the approach we present in this paper constitutes more of a syntactic reasoning on the source code level. For example, [4, Section 7] gives a circa two-page proof sketch of the expected run-time of a “simple random walk” carried out in PPDL. It requires a fair amount of domain-specific knowledge about integers and combinatorics and is thus not easily amenable to automation. A complete proof of the expected run-time in the **wp**-calculus à la McIver & Morgan requires only a fraction of the effort (see Appendix A). Partial automations of **wp**-style proofs in theorem provers such as Isabelle/HOL have been developed [10], [11]. A partial automation of **wp**-style proofs for expected run-times in the vein of [7] has recently been carried out by Hölzl [12]. The **wp**-style calculus for mixed-sign expectations we present here is closely related to the standard weakest pre-expectation calculus and so we believe that existing automation techniques are likely to carry over easily.

At first sight, avoiding mixed-sign expectations looks like a minor technical restriction. In practice it is not: For instance, program variables may become negative during program execution, having a negative impact of f ’s value. As another example, the efficiency of data structures such as randomized splay trees [13] is typically carried out using amortized analysis. Such analysis is similar to expected run-time analysis, but is concerned with the cost averaged over a sequence of operations. In the accounting and potential method in amortized analysis, a decrease in potential (or credit) “pays for” particularly expensive operations whereas increases model cheap operations. The amortized cost f during the execution of a probabilistic program may thus become arbitrarily negative. Finally, we mention that negative expectations or even negative probabilities have applications in quantum computing and finance.²

Current **wp**-approaches do not handle the aforementioned scenarios off-the-shelf. A workaround is to perform a Jordan decomposition of f by $f = {}^+f - {}^-f$, where ${}^+f$ and ${}^-f$ are both non-negative expectations, and analyze ${}^+f$ and ${}^-f$ individually using the standard **wp**-calculus. This, however, can easily become quite involved, for example when trying to

reason about the expected value of x after execution of

$$\text{while } (1/2) \{x := -x - \text{sign}(x)\} .$$

In every iteration, a fair coin is flipped to decide whether to terminate the loop or execute its body followed by a recursive execution of the entire loop. Intuitively, this program computes a variant of a geometric distribution on x where the sign alternates with increasing absolute value of x . The expected value of x after execution of the above program is given by $x/3 - \text{sign}(x)/9$. A detailed comparison of tackling this analysis by the methods presented in this paper to a Jordan-decomposition-based approach is provided in Appendix B.

Despite the existence of a mathematical theory of signed random variables, there are good reasons why they are avoided in current **wp**-approaches: the notion of expectation needs to be reconsidered, and a complete partial order on these adapted expectations—key to defining the semantics of loop programs—is required. It turns out that this is not trivial. It is this challenge that this paper attempts to take up. We provide a sound semantics of probabilistic programs that directly manipulates mixed-sign expectations f . In particular, *our semantics is always defined regardless of whether classical pre-expectations [4], [3], [6] exist or not*. We start by redefining what an expectation that can be negative in fact is. The crux of our approach is to keep track of the integrability of the mixed-sign random variable f by accompanying f with a non-negative (but possibly infinite) expectation g that bounds $|f|$. Notice that we *do not* require f to be integrable as we want our semantics to be well-defined regardless of whether f is integrable or not. Instead, our semantics internally keeps track of f ’s integrability. We obtain a partial order by considering the kernel of a quasi-order on pairs (f, g) . Equivalence classes under this kernel constitute the counterpart of expectations for the setting with mixed-sign random variables. This provides the basis for providing a sound **wp**-calculus for reasoning about probabilistic programs with mixed-sign expectations. In our setting, providing a sound semantics for loops cannot be done in the standard way, as Kleene’s fixed point theorem is not applicable. We therefore provide a direct proof. An important ingredient to make this work is proving the existence of unique limits of sequences of equivalence classes of pairs (f, g) . Moreover, we prove monotonicity and soundness of our novel weakest pre-expectation transformer. This all is accompanied by a proof rule for reasoning about loops. Various examples show the applicability of our transformer.

Organization of the paper: In Section 2, we present syntax and effects of the probabilistic programming language that we build upon. In Section 3, we revisit the traditional **wp**-calculus and investigate the problems that would occur when naively letting the calculus act on mixed-sign expectations. In Section 4, we present a new notion of mixed-sign expectations called *integrability-witnessing expectations*, which incorporate bookkeeping for the integrability of the expectations. In Section 5, we present a **wp**-calculus acting on integrability-witnessing expectations. In Section 6, we show that our calculus is sound and allows for monotonic reasoning.

²See https://en.wikipedia.org/wiki/Negative_probability and the various references therein.

Furthermore, we present an invariant rule for reasoning about loops and show its applicability. We conclude with Section 7.

II. THE PROBABILISTIC PROGRAMMING LANGUAGE

In this section we present the probabilistic programming language used throughout this paper. To model probabilistic programs we employ a standard imperative language à la Dijkstra's Guarded Command Language [2] with a probabilistic feature: we allow for the guards that guard if-then-else constructs and while-loops to be probabilistic. As an example, we allow for a program like

$$\text{while } (2/3 \cdot \langle x \text{ even} \rangle + 1/3 \cdot \langle x \text{ odd} \rangle) \{x := x + 1\}$$

which uses a probabilistic loop guard to establish a variant of a geometric distribution on the program variable x . With probability $2/3$ the loop *terminates* if x is odd and with probability $1/3$ the loop terminates if x is even.

Formally, the set of programs in the *probabilistic guarded command language*, denoted **pProgs**, is given by the grammar

$$\begin{aligned} C \quad \longrightarrow \quad & \text{skip} \mid x := E \mid C; C \\ & \mid \text{if } (\xi) \{C\} \text{ else } \{C\} \mid \text{while } (\xi) \{C\} . \end{aligned}$$

Here x is a *program variable* in Var , E an arithmetical expression over program variables and ξ a *probabilistic guard* in **PGuards**.

To describe the effect of the different language constructs we first present some preliminaries. A *program state* σ is a mapping from a finite set of program variables Var to a countable set of values Val . Let $\Sigma = \{\sigma \mid \sigma: \text{Var} \rightarrow \text{Val}\}$ denote the *set of program states*. We assume an interpretation function $\llbracket \cdot \rrbracket: \text{PGuards} \rightarrow \Sigma \rightarrow [0, 1]$ for probabilistic guards: $\llbracket \xi \rrbracket$ maps each program state to the probability that the guard evaluates to true. We write $\llbracket \neg \xi \rrbracket$ as a shorthand for $\lambda \sigma. 1 - \llbracket \xi \rrbracket(\sigma)$. E.g. $\llbracket x \geq y \rrbracket(\sigma)$ evaluates with probability 1 to true if $\sigma(x) \geq \sigma(y)$ and otherwise with probability 1 to false. As another example $\llbracket 1/2 \rrbracket(\sigma)$ evaluates with probability $1/2$ to true and with probability $1/2$ to false, regardless of σ .

We now present the effects of programs in **pProgs**. For that, let σ be the current program state. **skip** has no effect on the program state. $x := E$ is an assignment which evaluates expression E in the current program state and assigns this value to variable x . $C_1; C_2$ is the sequential composition of programs C_1 and C_2 , i.e. first C_1 is executed, then C_2 . $\text{if } (\xi) \{C_1\} \text{ else } \{C_2\}$ is a probabilistic conditional branching: C_1 is executed with probability $\llbracket \xi \rrbracket(\sigma)$ and C_2 with probability $1 - \llbracket \xi \rrbracket(\sigma)$. $\text{while } (\xi) \{C\}$ is a probabilistically guarded while loop: with probability $\llbracket \xi \rrbracket(\sigma)$ the loop body C is executed followed by a recursive execution of the loop, whereas with probability $1 - \llbracket \xi \rrbracket(\sigma)$ the loop terminates.

Example 1 (Tortoise and Hare [14]). The program

$$\begin{aligned} & t := 30; h := 0; \\ & \text{while } (h \leq t) \{ \\ & \quad t := t + 1; \\ & \quad \text{if } (1/2) \{h := h + 3\} \text{ else } \{\text{skip}\} \} \end{aligned}$$

illustrates the use of the programming language. It models a race between a tortoise and a hare (t and h represent their respective positions). The tortoise starts with a lead of 30 and advances one step forward in each round. The hare advances three steps or remains still, both with the remaining probability of $1/2$. The race ends when the hare passes the tortoise. \triangle

III. NON-NEGATIVE WEAKEST PRE-EXPECTATIONS

In this section, we recall the standard weakest pre-expectation semantics which acts on non-negative random variables. When we start a probabilistic program C in some initial state σ , the final state after termination of C need not be unique due to C 's probabilistic nature. In fact, not even the event of C 's termination itself needs to be determined as the program's computation might diverge with a probability that is neither 0 nor 1. So instead of thinking of C as a mapping from initial to final states, we can rather think of C as a mapping from a distribution μ_0 of initial states to a distribution $\llbracket C \rrbracket(\mu_0)$ of final states. In order to account for non-termination, we do not require the total probability mass of these distributions to sum up to 1 but any probability between 0 and 1 is valid. The missing probability mass represents then the probability of non-termination.

Given a random variable f mapping program states to *positive reals*, we can ask: What is the expected value of f after termination of C when the input to C is distributed according to μ_0 ? E.g., what is the expected value of h after termination of $\text{if } (1/2) \{h := h + 3\} \text{ else } \{\text{skip}\}$ on an initial distribution in which h is 4 with probability $2/3$ and h is 7 with probability $1/3$?

In this case, the answer is 6.5. In general, an answer to this type of questions can be obtained by means of the weakest pre-expectation calculus [4], [3], [15]: This calculus can be used to reason about the expected value of a random variable after termination of a probabilistic program C . More precisely, the weakest pre-expectation transformer $\text{wp}[C]$ transforms a given non-negative random variable f into a random variable $g = \text{wp}[C](f)$, such that for any initial distribution μ_0 the expected value of f under the *final* distribution $\llbracket C \rrbracket(\mu_0)$ coincides with the expected value of g under the *initial* distribution μ_0 .³ Put formally, we have

$$\mathbb{E}_{\mu_0}(\text{wp}[C](f)) = \mathbb{E}_{\llbracket C \rrbracket(\mu_0)}(f) , \quad (1)$$

where $\mathbb{E}_{\mu}(h)$ denotes the expected value of a random variable h under distribution μ . In particular, if the program C is started in a single determined initial state σ , then the expected value of f after termination of C on input σ is given by $\text{wp}[C](f)(\sigma)$, since $\text{wp}[C](f)(\sigma) = \mathbb{E}_{\delta_{\sigma}}(\text{wp}[C](f)) = \mathbb{E}_{\llbracket C \rrbracket(\delta_{\sigma})}(f)$, where δ_{σ} is the Dirac distribution that assigns the entire probability mass (i.e. 1) to the single point σ .

Notice that wp is not a distribution transformer per se. Nevertheless, given some predicate A , we can express the

³A correspondence between the operational point of view outlined in Section II and the denotational wp -semantics for probabilistic programs is provided in [15].

TABLE I
DEFINITIONS FOR THE \mathbf{wp} TRANSFORMER ACTING ON $\mathbb{E}_{\geq 0}^\infty$.

C	$\mathbf{wp}[C](f)$
<code>skip</code>	f
$x := E$	$f[x/E]$
$C_1; C_2$	$\mathbf{wp}[C_1](\mathbf{wp}[C_2](f))$
$\text{if } (\xi) \{C_1\} \text{ else } \{C_2\}$	$\llbracket \xi \rrbracket \cdot \mathbf{wp}[C_1](f) + \llbracket \neg \xi \rrbracket \cdot \mathbf{wp}[C_2](f)$
$\text{while } (\xi) \{C'\}$	$\text{lfp } X \bullet \llbracket \neg \xi \rrbracket \cdot f + \llbracket \xi \rrbracket \cdot \mathbf{wp}[C'](X)$

probability that C terminates on initial state σ in some state satisfying A in terms of \mathbf{wp} by $\mathbf{wp}[C](\llbracket A \rrbracket)(\sigma)$, where $\llbracket A \rrbracket$ is the indicator function of predicate A .

In the context of the weakest pre-expectation calculus, random variables are usually referred to as *expectations*: f is called the *post-expectation* and $g = \mathbf{wp}[C](f)$ is called the *pre-expectation*.⁴ The set of expectations is denoted by

$$\mathbb{E}_{\geq 0}^\infty = \{f \mid f: \Sigma \rightarrow \mathbb{R}_{\geq 0}^\infty\},$$

where $\mathbb{R}_{\geq 0}^\infty = \{r \in \mathbb{R} \mid r \geq 0\} \cup \{\infty\}$. We need the extended real line here, as we want $\mathbf{wp}[C](f)$ to always be defined for any $C \in \mathbf{pProgs}$ and any $f \in \mathbb{E}_{\geq 0}^\infty$ and the expected value of f after termination of C can easily become infinity. Notice that for a probabilistic guard ξ , formally both $\llbracket \xi \rrbracket$ and $\llbracket \neg \xi \rrbracket$ are expectations as e.g. $\llbracket \xi \rrbracket: \Sigma \rightarrow [0, 1]$ and so $\llbracket \xi \rrbracket \in \mathbb{E}_{\geq 0}^\infty$.

Remark 1 (Positivity of Expectations). Since we have restricted ourselves to non-negative random variables in $\mathbb{E}_{\geq 0}^\infty$, the expected value in Equation (1) is always a well-defined positive real or $+\infty$ for any initial distribution. \triangle

The weakest pre-expectation transformer $\mathbf{wp}[C]$ can be defined by induction on the structure of the program C according to Table I. Let us briefly go over these definitions: $\mathbf{wp}[\text{skip}]$ behaves as the identity since `skip` does not modify the program state. For $\mathbf{wp}[x := E](f)$ we return $f[x/E]$ which is obtained from f by a sort of “syntactic replacement” of x by E , just as in Hoare logic. More formally, $f[x/E] = \lambda \sigma \bullet f(\sigma[x \mapsto \sigma(E)])$. $\mathbf{wp}[C_1; C_2](f)$ obtains a pre-expectation for the program $C_1; C_2$ by applying $\mathbf{wp}[C_1]$ to the intermediate expectation obtained from $\mathbf{wp}[C_2](f)$. $\mathbf{wp}[\text{if } (\xi) \{C_1\} \text{ else } \{C_2\}](f)$ weights $\mathbf{wp}[C_1](f)$ and $\mathbf{wp}[C_2](f)$ according to the probability of the guard evaluating to true and false. Addition and multiplication of expectations is meant pointwise here, so $f + g = \lambda \sigma \bullet f(\sigma) + g(\sigma)$ and $f \cdot g = \lambda \sigma \bullet f(\sigma) \cdot g(\sigma)$. Before we turn to the definitions for while-loops, let us illustrate the effects of the \mathbf{wp} transformer by means of an example:

Example 2 (Truncated Geometric Distribution). Consider the following probabilistic program:

$$C_{\text{trunc}}: \text{if } (1/2) \{ \text{skip} \} \text{ else } \{ \\ x := x + 1; \}$$

⁴As the *postexpectation* is evaluated in the *final* states and the *preexpectation* is evaluated in the *initial* states.

$$\text{if } (1/2) \{ \text{skip} \} \text{ else } \{ x := x + 1 \}$$

It can be viewed as modeling a truncated geometric distribution: we repeatedly flip a fair coin until observing the first, say, heads or completing the second unsuccessful trial. Suppose we want to know the expected value of x . Then we can calculate this by calculating $\mathbf{wp}[C_{\text{trunc}}](x)$ as follows:⁵

$$\begin{aligned} \mathbf{wp}[C_{\text{trunc}}](x) &= \frac{1}{2} \cdot \mathbf{wp}[\text{skip}](x) + \frac{1}{2} \cdot \mathbf{wp}[\dots; \dots](x) \\ &= \frac{x}{2} + \frac{1}{2} \cdot \mathbf{wp}[x := x + 1] \left(\frac{1}{2} \cdot \mathbf{wp}[\text{skip}](x) \right. \\ &\quad \left. + \frac{1}{2} \cdot \mathbf{wp}[x := x + 1](x) \right) \\ &= \frac{x}{2} + \frac{1}{2} \cdot \mathbf{wp}[x := x + 1] \left(\frac{x}{2} + \frac{x+1}{2} \right) \\ &= \frac{x}{2} + \frac{x+1}{4} + \frac{x+2}{4} = x + \frac{3}{4} \end{aligned}$$

Therefore, the expected value of x after execution of C_{trunc} is $x + 3/4$, where $x + 3/4$ is to be evaluated in the initial state in which C_{trunc} is started. \triangle

We now turn to weakest pre-expectations of while-loops. While the calculation of \mathbf{wp} in the above example was straightforward as the program C_{trunc} is loop-free, \mathbf{wp} of while-loops is defined using fixed point techniques. For that, we need a complete partial order $(\mathbb{E}_{\geq 0}^\infty, \leq)$ which is given by

$$f \leq g \quad \text{iff} \quad \forall \sigma: f(\sigma) \leq g(\sigma).$$

The bottom element of this complete partial order is given by the constantly zero expectation $\mathbf{0} = \lambda \sigma \bullet 0$. The supremum is taken pointwise, so for any subset $D \subseteq \mathbb{E}_{\geq 0}^\infty$, $\sup D = \lambda \sigma \bullet \sup_{f \in D} f(\sigma)$. Notice that this pointwise supremum always exists as any bounded set of real numbers has a supremum and $+\infty$ is a valid supremum of unbounded sets. Thus $(\mathbb{E}_{\geq 0}^\infty, \leq)$ is indeed a *complete* partial order with bottom element $\mathbf{0}$. (It is even a complete lattice.)

Using this complete partial order, the weakest pre-expectation of a while-loop $\text{while } (\xi) \{C'\}$ is then given in terms of the least fixed point of a special transformer $C'^\xi F_f: \mathbb{E}_{\geq 0}^\infty \rightarrow \mathbb{E}_{\geq 0}^\infty$ constructed from the loop guard ξ , the postexpectation f , and the \mathbf{wp} transformer of the loop body $\mathbf{wp}[C']$ (see Table I). The transformer $C'^\xi F_f$ is given by

$$C'^\xi F_f(X) = \llbracket \neg \xi \rrbracket \cdot f + \llbracket \xi \rrbracket \cdot \mathbf{wp}[C'](X).$$

We call this transformer $C'^\xi F_f$ the *characteristic functional* of $\text{while } (\xi) \{C'\}$ with respect to post-expectation f . The existence of the least fixed point of $C'^\xi F_f$ is ensured by a standard denotational semantics argument (see e.g. [16, Ch. 5]), namely Scott-continuity (or simply continuity) of $C'^\xi F_f$ which follows from continuity of $\mathbf{wp}[C']$. By completeness of the partial order $(\mathbb{E}_{\geq 0}^\infty, \leq)$ and continuity of the transformer $C'^\xi F_f$, the

⁵We have overloaded the notation x that actually denotes the program variable x to the expectation $\lambda \sigma \bullet \sigma(x)$ for the sake of readability.

Kleene Fixed Point Theorem [17], [18] gives an even stronger result than mere existence of a least fixed point. It states that this least fixed point can be constructed in ω steps by iterated application of $C_f^\xi F_f$ to the least element $\mathbf{0}$, i.e.

$$\text{lfp}_{C_f^\xi F_f} = \sup_{n \in \mathbb{N}} C_f^\xi F_f^n(\mathbf{0}) ,$$

where $C_f^\xi F_f^n$ stands for n -fold application of $C_f^\xi F_f$ to its argument. As mentioned, this result holds only for continuous functions. Continuity of $\text{wp}[C]$ can be shown by structural induction on the structure of C in case C is not a loop and fixed point induction in case that C is a loop. Besides continuity, the wp transformer enjoys several other useful properties:

Theorem 1 (Properties of wp Acting on $\mathbb{E}_{\geq 0}^\infty$ [4], [3], [5]). *For any program $C \in \text{pProgs}$ the following properties hold:*

(1) **Continuity:** For any subset of expectations $D \subseteq \mathbb{E}_{\geq 0}^\infty$:

$$\text{wp}[C](\sup D) = \sup_{f \in D} \text{wp}[C](f)$$

(2) **Monotonicity:** For any two expectations $f, g \in \mathbb{E}_{\geq 0}^\infty$:

$$f \leq g \text{ implies } \text{wp}[C](f) \leq \text{wp}[C](g)$$

(3) **Linearity:** For any two expectations $f, g \in \mathbb{E}_{\geq 0}^\infty$ and any constant $r \in \mathbb{R}_{\geq 0}$:

$$\text{wp}[C](f + r \cdot g) = \text{wp}[C](f) + r \cdot \text{wp}[C](g)$$

(4) **Upper Loop Invariants:** For any expectation $I \in \mathbb{E}_{\geq 0}^\infty$:

$$C_f^\xi(I) \leq I \text{ implies } \text{wp}[\text{while}(\xi)\{C\}](f) \leq I$$

(5) **Lower Loop Invariants:** For any sequence of expectations $(I_n)_{n \in \mathbb{N}} \subseteq \mathbb{E}_{\geq 0}^\infty$:

$$I_0 \leq C_f^\xi(\mathbf{0}) \text{ and } I_{n+1} \leq C_f^\xi(I_n) \\ \text{implies } \sup_{n \in \mathbb{N}} I_n \leq \text{wp}[\text{while}(\xi)\{C\}](f)$$

We saw that wp is well-defined and enjoys several useful properties if we deal only with positive expectations (recall Remark 1). When dealing with expected values of mixed-sign random variables, things become much more intricate, even in classical probability theory where no computational aspects are considered. In the next section, we show how the wp calculus can be extended to act on mixed-sign expectations.

IV. INTEGRABILITY-WITNESSING EXPECTATIONS

In this section we outline some problems that occur when dealing with mixed-sign expectations and present our idea on how to circumvent them by incorporating a mechanism that keeps track of the integrability of the expectations.

A. Convergence and Definedness Issues

So far we had our wp -transformer act on the set $\mathbb{E}_{\geq 0}^\infty$ of positive valued expectations. For expectations that may also take negative values, the expected value after program termination might not be defined for different reasons. In the following, we present two problematic examples.

a) *Indefinite Divergence:* As a first example, we adopt a counterexample from McIver & Morgan [3]: Consider the mixed-sign random variable $f = (-2)^x$. The expected value of f after execution of C_{geo} , given by

$$C_{geo}: x := 1; \text{while}(1/2)\{x := x + 1\} ,$$

on an arbitrary initial state is described by the series⁶

$$S = \sum_{i=1}^{\infty} \frac{(-2)^i}{2^i} = -1 + 1 - 1 + 1 - 1 + \dots ,$$

which is indefinitely divergent, i.e. it neither converges to any real value nor does it tend to $+\infty$ or $-\infty$. Furthermore, the summands of this series can be reordered in such ways that the series tends to $+\infty$ or that it tends to $-\infty$. In any case, there exists no meaningful and in particular no *unique* expected value of f and thus no classical pre-expectation $\text{wp}[C_{geo}](f)$.

If we were to naively apply the standard weakest pre-expectation calculus, we would first obtain a pre-expectation for the loop, by constructing the characteristic functional

$$F(X) := \sum_{x:=x+1}^{1/2} F_{(-2)^x}(X) = \frac{(-2)^x}{2} + \frac{X[x/x+1]}{2}$$

and then doing fixed point iteration, i.e. iteratively apply F to $\mathbf{0}$. In doing so, we get the sequence

$$F(\mathbf{0}) = \frac{(-2)^x}{2} \\ F^2(\mathbf{0}) = \frac{(-2)^x}{2} + \frac{(-2)^{x+1}}{4} \\ F^3(\mathbf{0}) = \frac{(-2)^x}{2} + \frac{(-2)^{x+1}}{4} + \frac{(-2)^{x+2}}{8}$$

and so on. Notice, that the sequence $(F^n(\mathbf{0}))_{n \in \mathbb{N}}$ is not monotonically increasing, so iteratively applying F to $\mathbf{0}$ does not yield an ascending chain. If we nevertheless took the limit of this sequence—naively assuming it exists—, we would get

$$F^\omega(\mathbf{0}) = \sum_{i=0}^{\omega} \frac{(-2)^{x+i}}{2^{i+1}} .$$

Finally, we have to apply the wp -semantics of the assignment preceding the while-loop to $F^\omega(\mathbf{0})$, i.e. we have to calculate $\text{wp}[x := 1](F^\omega(\mathbf{0}))$, which gives

$$\sum_{i=0}^{\omega} \frac{(-2)^{i+1}}{2^{i+1}} = -1 + 1 - 1 + 1 - 1 + \dots .$$

This is not well-defined and hence we see that the standard wp cannot be applied to this example as is.

b) *Non-Absolute Convergence:* As a second example, consider the expected value of the mixed-sign random variable $f' = (-2)^x/x$ after executing C_{geo} . It is described by the series⁷

$$S' = \sum_{i=1}^{\infty} \frac{(-2)^i}{2^i \cdot i} = -1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \dots .$$

⁶ $\sum_{v \in \text{Val}} \text{Pr}_{\llbracket C_{geo} \rrbracket(\delta_\sigma)}(v) \cdot f(v) = \sum_{i=1}^{\infty} \frac{(-2)^i}{2^i} .$

⁷ $\sum_{v \in \text{Val}} \text{Pr}_{\llbracket C_{geo} \rrbracket(\delta_\sigma)}(v) \cdot f'(v) = \sum_{i=1}^{\infty} \frac{(-2)^i}{2^i \cdot i} .$

This series in this particular ordering converges to $-\ln(2)$.

Again, if we were to naively apply the standard weakest pre-expectation calculus, we would first obtain a pre-expectation for the loop, by constructing the characteristic functional

$$F'(X) := \text{wp}[x := x+1]^{1/2} F_{(-2)^x/x}(X) = \frac{(-2)^x}{2 \cdot x} + \frac{X[x/x+1]}{2}$$

and then do fixed point iteration, i.e. iteratively apply F' to $\mathbf{0}$. This yields

$$\begin{aligned} F'(\mathbf{0}) &= \frac{(-2)^x}{2 \cdot x} \\ F'^2(\mathbf{0}) &= \frac{(-2)^x}{2 \cdot x} + \frac{(-2)^{x+1}}{4 \cdot (x+1)} \\ F'^3(\mathbf{0}) &= \frac{(-2)^x}{2 \cdot x} + \frac{(-2)^{x+1}}{4 \cdot (x+1)} + \frac{(-2)^{x+2}}{8 \cdot (x+2)} \end{aligned}$$

and so on. Notice that, again, the sequence $(F'^n(\mathbf{0}))_{n \in \mathbb{N}}$ is *not* monotonically increasing, so iteratively applying F' to $\mathbf{0}$ does not yield an ascending chain. If we nevertheless take the limit of this sequence—again just assuming it exists—, we get

$$F'^\omega(\mathbf{0}) = \sum_{i=0}^{\omega} \frac{(-2)^{x+i}}{2^{i+1} \cdot (x+i)}.$$

Finally, we have to calculate $\text{wp}[x := 1](F'^\omega(\mathbf{0}))$, which gives

$$\sum_{i=0}^{\omega} \frac{(-2)^{i+1}}{2^{i+1} \cdot (1+i)} = -1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \dots,$$

and converges to $-\ln(2)$.

The reason that this example is nevertheless problematic is that by the well-known Riemann Series Theorem [19], the series S' can be reordered in such a fashion that the series converges to any value in $\mathbb{R} \cup \{-\infty, +\infty\}$. This is because the series does converge but not absolutely. A series $\sum_{i=0}^{\infty} a_i$ is said to *converge absolutely* if $\sum_{i=0}^{\infty} |a_i|$ converges. If a series is absolutely convergent, then the series is also unconditionally convergent, meaning that the series converges to a unique value regardless of how the summands are ordered. If, however, a series converges non-absolutely, then the Riemann Series Theorem states that its summands can always be reordered in such a way that the series converges to an arbitrary value or that it tends to $+\infty$ or that it tends to $-\infty$.

This behavior of non-absolutely convergent series under reordering is highly undesirable for expected values since the outcomes of random events are only assigned a probability, and there exists no natural ordering of the summands in which their weighted masses should be summed up to an expected value. This is the reason why in classical probability theory the expected value $E_\mu(f)$ of a mixed-sign random variable f is only defined if $E_\mu(|f|) < \infty$, because that condition is exactly what ensures absolute convergence of the series representing $E_\mu(f)$. Next, we investigate how to incorporate the notion of absolute convergence into a new notion for mixed-sign expectations.

B. Integrability–Witnessing Expectations

If a random variable f fulfills the condition $E_\mu(|f|) < \infty$, then f is called *integrable*. Our goal is to formally incorporate the bookkeeping whether f is integrable or not into the objects on which a new weakest pre-expectation calculus acts in order to obtain a sound calculus for mixed-sign expectations. The first thing on our path to this goal is to alter our expectation space to allow for random variables to evaluate to both positive and negative reals.

Definition 1 (Mixed–Sign Expectations). The set \mathbb{E}^* of mixed-sign expectations (or simply expectations) is given by

$$\mathbb{E}^* = \{f \mid f: \Sigma \rightarrow \mathbb{R}\}. \quad \triangle$$

Notice that we have dropped the ∞ element from the codomain of an expectation, since if f is integrable, then the expected value of f is finite anyway.

Next, we present our integrability bookkeeping approach. The idea for keeping track of the integrability of an expectation f is to keep a pair of expectations (f, g) where g is a *non-negative* expectation that bounds $|f|$. We call such a pair an *integrability–witnessing pair*. The idea is that pre-expectations are computed for both components simultaneously.

Definition 2 (Integrability–Witnessing Pairs). The set \mathbb{P} of integrability–witnessing pairs is defined as a set of pairs

$$\mathbb{P} = \{(f, g) \mid f \in \mathbb{E}^*, g \in \mathbb{E}_{\geq 0}^\infty, |f| \leq g\}.$$

We define addition of two integrability–witnessing pairs by $(f, g) + (f', g') = (f + f', g + g')$, a scalar multiplication by $c \cdot (f, g) = (c \cdot f, |c| \cdot g)$ for $c \in \mathbb{R}$, and a multiplication by $h \cdot (f, g) = (h \cdot f, |h| \cdot g)$, for $h \in \mathbb{E}^*$. \triangle

Next, we would like to define an ordering on integrability–witnessing pairs. We would like to compare pairs component-wise, i.e. (f, g) should be less or equal (f', g') if both $f \leq f'$ and $g \leq g'$. This would naturally extend the complete partial order \leq on $\mathbb{E}_{\geq 0}^\infty$ to \mathbb{P} . There is, however, a catch:

Recall that the intuition behind a pair (f, g) is that whenever the expected value of g is finite, then the expected value of $|f|$, too, is finite by monotonicity of the expected value operator. If the expected value of g is infinity, however, then the expected value of f cannot be ensured to be defined. (In particular, if $g = |f|$, then the expected value of f should definitely be undefined.) Therefore, if g' is the pre-expectation of g and for a state $\sigma \in \Sigma$ we have $g'(\sigma) = \infty$, then we should not care about the pre-expectation of f in state σ since definedness cannot be ensured. This consideration should be reflected in our order on \mathbb{P} : For states where the second component evaluates to ∞ , the first component should not be compared. This gives rise to the following definition:

Definition 3 (The Quasi-Order \lesssim on \mathbb{P}). A quasi-order (\mathbb{P}, \lesssim) is given by

$$(f, g) \lesssim (f', g')$$

iff for all $\sigma \in \Sigma$,

$$g'(\sigma) \neq \infty \text{ implies } f(\sigma) \leq f'(\sigma) \text{ and } g(\sigma) \leq g'(\sigma). \quad \triangle$$

In contrast to a partial order which is reflexive, transitive and antisymmetric, in a quasi-order the requirement of antisymmetry is dropped. Notice that, indeed, \lesssim is only a quasi-order since we can have two integrability-witnessing pairs (f, g) and (f', g') such that for some state $\sigma \in \Sigma$ we have $g(\sigma) = \infty = g'(\sigma)$, but $f(\sigma) \neq f'(\sigma)$, and so $(f, g) \neq (f', g')$. Still (f, g) and (f', g') compare in both directions, so we have $(f, g) \lesssim (f', g')$ and $(f, g) \gtrsim (f', g')$, but not $(f, g) = (f', g')$. This leads us to finding that \lesssim is *not antisymmetric*.

On the other hand, two integrability-witnessing pairs (f, g) and (f', g') , for which $f(\sigma) \neq f'(\sigma)$ holds only for those states in which $g(\sigma) = \infty = g'(\sigma)$, should be considered *equivalent*, even though they are not equal. This is because for states σ in which $g(\sigma) = \infty = g'(\sigma)$, the evaluations of $f(\sigma)$ and $f'(\sigma)$ are ignored since integrability is not ensured. Consequently, we need a notion of equivalence of integrability-witnessing pairs:

Definition 4 (Integrability-Witnessing Expectations). The quasi-order \lesssim induces a canonical [18] equivalence relation \approx , given by $\approx = \lesssim \cap \gtrsim$, i.e.

$$(f, g) \approx (f', g')$$

iff for all $\sigma \in \Sigma$,

$$\begin{aligned} &g(\sigma) \neq \infty \text{ or } g'(\sigma) \neq \infty \\ &\text{implies } f(\sigma) = f'(\sigma) \text{ and } g(\sigma) = g'(\sigma). \end{aligned}$$

We denote by $\lfloor f, g \rfloor$ or simply $\lfloor f, g \rfloor$ the equivalence class of (f, g) under \approx and call such an equivalence class an *integrability-witnessing expectation*. We denote by \mathbb{IE} the set of integrability-witnessing expectations, i.e. the set of equivalence classes of \approx . \triangle

Intuitively, an equivalence class $\lfloor f, g \rfloor$ can be thought of as a particular pair (f, g) such that g maps each state either to a non-negative real number or ∞ and f maps each state that is not mapped to ∞ by g to a real number.

Notice that we call the equivalence classes and not the pairs “expectations” as we consider \mathbb{IE} and not \mathbb{P} to be a suitable domain to perform computations on and thus we consider \mathbb{IE} to be the mixed-sign counterpart to $\mathbb{E}_{\geq 0}^\infty$. Next, we define a *partial order on the equivalence classes*:

Definition 5 (The Partial Order on \mathbb{IE}). The quasi-order \lesssim on the set \mathbb{P} of integrability-witnessing pairs induces a canonical [18] partial order \sqsubseteq on the set \mathbb{IE} of integrability-witnessing expectations by

$$\lfloor f_1, g_1 \rfloor \sqsubseteq \lfloor f_2, g_2 \rfloor \text{ iff } (f_1, g_1) \lesssim (f_2, g_2). \quad \triangle$$

As for an intuitive interpretation of this partial order, we note that if $\lfloor f_1, g_1 \rfloor \sqsubseteq \lfloor f_2, g_2 \rfloor$ holds, then we have $f'_1(\sigma) = f_1(\sigma) \leq f_2(\sigma) = f'_2(\sigma)$ for all $(f'_1, g'_1) \in \lfloor f_1, g_1 \rfloor$, $(f'_2, g'_2) \in \lfloor f_2, g_2 \rfloor$, and all states σ in which $g_2(\sigma) \neq \infty$ holds. Thus if integrability in σ is ensured, the first components compare in σ , which is the comparison we are mainly interested in.

The partial order \sqsubseteq on \mathbb{IE} is complete in the sense that every *non-empty* subset $D \subseteq \mathbb{IE}$ has a supremum $\sup D = \lfloor \hat{f}, \hat{g} \rfloor$ given by

$$\begin{aligned} \hat{g}(\sigma) &= \sup \{g(\sigma) \mid (f, g) \in \lfloor f, g \rfloor \in D\} \\ \hat{f}(\sigma) &= \begin{cases} \sup \{f(\sigma) \mid (f, g) \in \lfloor f, g \rfloor \in D\}, & \text{if } \hat{g}(\sigma) \neq \infty, \\ 0, & \text{otherwise,}^8 \end{cases} \end{aligned}$$

where ∞ is assumed to be a valid supremum for $\hat{g}(\sigma)$.

An unfortunate fact about the partial order $(\mathbb{IE}, \sqsubseteq)$ is that it has *no least element*. In particular $\lfloor 0, 0 \rfloor$ is not a least element of \mathbb{IE} since, for example $\lfloor 0, 0 \rfloor \not\sqsubseteq \lfloor -1, 1 \rfloor$, where $-1 = \lambda\sigma \bullet -1$ and $1 = \lambda\sigma \bullet 1$. This fact prevents us from applying the Kleene Fixed Point Theorem—as is typically done in **wp**-calculi—in our later development.

In the next section, we investigate a weakest pre-expectation calculus acting on integrability-witnessing expectations.

V. MIXED-SIGN WEAKEST PRE-EXPECTATIONS

We now develop a weakest pre-expectation calculus acting on integrability-witnessing expectations. For that we first observe that certain operations on an integrability-witnessing pair (f, g) preserve \approx -equivalence and thus lifting this operation to the integrability-witnessing expectation $\lfloor f, g \rfloor$ can be done by performing the operation on the representative (f, g) and then taking the equivalence class of the resulting pair.

E.g., the assignment $x := E$ preserves \approx -equivalence, since if $(f, g) \approx (f', g')$ then for all $\sigma \in \Sigma$ we have

$$\begin{aligned} &g(\sigma) \neq \infty \text{ or } \infty \neq g'(\sigma) \\ &\text{implies } f(\sigma) = f'(\sigma) \text{ and } g(\sigma) = g'(\sigma). \end{aligned}$$

But then this is in particular true for all updated states of the form $\sigma[x \mapsto \sigma(E)]$ and thus \approx -equivalence is preserved by the assignment, i.e.

$$\begin{aligned} &(f, g) \approx (f', g') \\ &\text{implies } (f[x/E], g[x/E]) \approx (f'[x/E], g'[x/E]). \end{aligned}$$

Moreover this allows for defining a transformer

$$\widetilde{\text{wp}}[x := E] \lfloor f, g \rfloor = \lfloor f[x/E], g[x/E] \rfloor.$$

Furthermore, one can show that addition, scalar multiplication, and multiplication also preserve \approx -equivalence. This puts us in a position to formally define a weakest pre-expectation transformer acting on \mathbb{IE} :

Definition 6 (The Transformer $\widetilde{\text{wp}}$). The transformer $\widetilde{\text{wp}}[C]: \mathbb{IE} \rightarrow \mathbb{IE}$ is defined by induction on the structure of C according to Table II. \triangle

Let us briefly go over these definitions: Just like $\text{wp}[\text{skip}]$, $\widetilde{\text{wp}}[\text{skip}]$ is an identity since skip does not modify the program state. $\widetilde{\text{wp}}[x := E] \lfloor f, g \rfloor$ takes a representative $(f, g) \in$

⁸Notice that this 0 is an arbitrary choice of a value in \mathbb{R} since any (\hat{f}', \hat{g}) , where $\hat{f}'(\sigma) \neq 0$ for any $\sigma \in \Sigma$ with $\hat{g}(\sigma) = \infty$, is in the same equivalence class as (\hat{f}, \hat{g}) .

TABLE II
DEFINITIONS FOR THE $\widetilde{\mathbf{wp}}$ TRANSFORMER ACTING ON \mathbb{IE} .

C	$\widetilde{\mathbf{wp}}[C]\{f, g\}$
<code>skip</code>	$\{f, g\}$
$x := E$	$\{f[x/E], g[x/E]\}$
$C_1; C_2$	$\widetilde{\mathbf{wp}}[C_1](\widetilde{\mathbf{wp}}[C_2]\{f, g\})$
<code>if</code> $(\xi)\{C_1\} else \{C_2\}$	$\llbracket \xi \rrbracket \cdot \widetilde{\mathbf{wp}}[C_1]\{f, g\} + \llbracket \neg \xi \rrbracket \cdot \widetilde{\mathbf{wp}}[C_2]\{f, g\}$
<code>while</code> $(\xi)\{C'\}$	$\lim_{n \rightarrow \omega} {}^\xi F_{C', g}^n \{0, 0\}$
${}^\xi F_{\{f, g\}}^n \{X, Y\} = \llbracket \neg \xi \rrbracket \cdot \{f, g\} + \llbracket \xi \rrbracket \cdot \widetilde{\mathbf{wp}}[C]\{X, Y\}$	

$\{f, g\}$, performs the assignment $x := E$ on both components to obtain $(f[x/E], g[x/E])$ and then returns the corresponding equivalence class $\{f[x/E], g[x/E]\}$. As described earlier, assignments preserve \approx -equivalence, so doing the update on the representative is a sound and sufficient course of action.

$\widetilde{\mathbf{wp}}[C_1; C_2]\{f, g\}$ obtains a pre-expectation for $C_1; C_2$ by applying $\widetilde{\mathbf{wp}}[C_1]$ to the intermediate integrability-witnessing expectation obtained from $\widetilde{\mathbf{wp}}[C_2]\{f, g\}$. $\widetilde{\mathbf{wp}}[\text{if } (\xi)\{C_1\} \text{ else } \{C_2\}]\{f, g\}$ weights $\widetilde{\mathbf{wp}}[C_1]\{f, g\}$ and $\widetilde{\mathbf{wp}}[C_2]\{f, g\}$ according to the probability of the guard ξ evaluating to true and false by multiplication and addition on integrability-witnessing expectations (see Definition 2).

Before we turn our attention to the definitions of $\widetilde{\mathbf{wp}}$ for while-loops, let us illustrate the effects of the $\widetilde{\mathbf{wp}}$ transformer by means of a variation of Example 2:

Example 3 (Truncated Alternating Geometric Distribution). Consider the probabilistic program $C_{alttrunc}$:

$C_{alttrunc}$: `if` $(1/2)\{\text{skip}\} `else` $\{$
 $x := -x - 1;$
`if` $(1/2)\{\text{skip}\} `else` $\{x := -x + 1\}\}$$$

It is a variant of C_{trunc} from Example 2 where the program alternates the sign of x and also alternates the sign of the change in x . Suppose we want to know the expected value of x after termination of $C_{alttrunc}$. The according integrability-witnessing post-expectation for obtaining an answer to this question is $\{x, |x|\}$. Notice that in this example, the need for mixed-sign random variables arises *not* from some artificially constructed mixed-sign post-expectation but *directly from the program code*. In order to reason about the expected value of x after termination, we calculate $\widetilde{\mathbf{wp}}[C_{alttrunc}]\{x, |x|\}$:

$$\begin{aligned} & \widetilde{\mathbf{wp}}[C_{alttrunc}]\{x, |x|\} \\ &= \frac{1}{2} \cdot \widetilde{\mathbf{wp}}[\text{skip}]\{x, |x|\} + \frac{1}{2} \cdot \widetilde{\mathbf{wp}}[\dots; \dots]\{x, |x|\} \\ &= \frac{1}{2} \cdot \{x, |x|\} + \frac{1}{2} \cdot \widetilde{\mathbf{wp}}[\dots] \left(\frac{1}{2} \cdot \widetilde{\mathbf{wp}}[\text{skip}]\{x, |x|\} \right. \\ & \quad \left. + \frac{1}{2} \cdot \widetilde{\mathbf{wp}}[x := -x + 1]\{x, |x|\} \right) \end{aligned}$$

$$\begin{aligned} &= \{ \frac{x}{2}, \frac{|x|}{2} \} + \frac{1}{2} \cdot \widetilde{\mathbf{wp}}[x := -x - 1] \left(\frac{1}{2} \cdot \{x, |x|\} \right. \\ & \quad \left. + \frac{1}{2} \cdot \{-x + 1, |-x + 1|\} \right) \\ &= \{ \frac{x}{2}, \frac{|x|}{2} \} + \{ \frac{-x - 1}{4}, \frac{|x + 1|}{4} \} \\ & \quad + \{ \frac{x + 2}{4}, \frac{|x + 2|}{4} \} \\ &= \{ \frac{x}{2} + \frac{1}{4}, \frac{2 \cdot |x| + |x + 1| + |x + 2|}{4} \} \end{aligned}$$

The first observation we can make from this result is that the expected value of x is defined after execution of $C_{alttrunc}$, since in every initial state we have $2 \cdot |x| + |x + 1| + |x + 2|/4 < \infty$. The second observation we can make is that this expected value is for every initial state given by $x/2 + \frac{1}{4}$, which is to be evaluated in the initial state in which $C_{alttrunc}$ is started. In particular, the above expression gives the correct expected value, *regardless* of whether the program is started with a positive or negative variable valuation for x . \triangle

We now turn towards weakest pre-expectations of *while-loops*. While the calculation of $\widetilde{\mathbf{wp}}$ in the above example was straightforward as the program $C_{alttrunc}$ is loop-free, $\widetilde{\mathbf{wp}}$ of while-loops is defined using a limit construct. For that we first need to formally define what a limit of a sequence of integrability-witnessing expectations, i.e. a limit of a sequence of equivalence classes, is.

Definition 7 (Limits of Sequences in \mathbb{IE}). Let $(\{f_n, g_n\})_{n \in \mathbb{N}} \subseteq \mathbb{IE}$ be a sequence in \mathbb{IE} . Then

$$\{f, g\} \text{ is a limit of } (\{f_n, g_n\})_{n \in \mathbb{N}},$$

if there exists a sequence $((f'_n, g'_n))_{n \in \mathbb{N}}$ of representatives, i.e. for all $n \in \mathbb{N}$, $(f'_n, g'_n) \in \{f_n, g_n\}$, with

$$f(\sigma) = \begin{cases} \lim_{n \rightarrow \omega} f'_n(\sigma), & \text{if } \lim_{n \rightarrow \omega} g'_n(\sigma) \neq \infty, \\ 0, & \text{otherwise,}^9 \text{ and} \end{cases}$$

$$g(\sigma) = \lim_{n \rightarrow \omega} g'_n(\sigma),$$

where ∞ is assumed to be a valid limit for $g'_n(\sigma)$. \triangle

The intuition behind this definition is that a limit of a sequence in \mathbb{IE} is a pointwise limit (in each state $\sigma \in \Sigma$).

If a limit exists, we note the following: For each pair in any equivalence class, the second component is unique. Thus the sequence $(g'_n)_{n \in \mathbb{N}}$ is uniquely determined by $(g_n)_{n \in \mathbb{N}}$.

Now, if $\lim_{n \rightarrow \infty} g_n(\sigma) = \infty$, then the limit in that state σ does not depend on the sequence $(f'_n)_{n \in \mathbb{N}}$ and is uniquely determined. If on the other hand $\lim_{n \rightarrow \infty} g_n(\sigma) \neq \infty$, then for almost all g_i we have $g_i(\sigma) \neq \infty$ and thus also almost all f'_i are uniquely determined by f_i . All in all this leads to the fact that if a limit of $(\{f_n, g_n\})_{n \in \mathbb{N}}$ exists, then we

⁹Notice that this 0 is again an arbitrary choice of a value in \mathbb{R} since any (f', g) , where $f'(\sigma) \neq 0$ for any $\sigma \in \Sigma$ with $g(\sigma) = \infty$, is in the same equivalence class as (f, g) . See also Footnote 8.

can reason about the existence by means of the sequence of representatives $((f_n, g_n))_{n \in \mathbb{N}}$.

The $\widetilde{\mathbf{wp}}$ -semantics of while-loops is defined as the limit of a sequence of integrability-witnessing expectations, but in order to speak of *the* limit, such limits must be unique if they exist. This is ensured by the following theorem:

Theorem 2 (Uniqueness of Limits in \mathbb{IE}). *Let $(\langle f_n, g_n \rangle)_{n \in \mathbb{N}} \subseteq \mathbb{IE}$ and let a limit of that sequence exist. Then that limit is unique, i.e. if $\langle f, g \rangle$ and $\langle f', g' \rangle$ are both a limit of $\langle f_n, g_n \rangle$, then $\langle f, g \rangle = \langle f', g' \rangle$.*

Proof. Suppose for a contradiction that $\langle f, g \rangle \neq \langle f', g' \rangle$ are both a limit of the sequence $(\langle f_n, g_n \rangle)_{n \in \mathbb{N}} \subseteq \mathbb{IE}$. Recall that we can reason about such a limit entirely by the sequence of representatives $((f_n, g_n))_{n \in \mathbb{N}}$. Because of $\langle f, g \rangle \neq \langle f', g' \rangle$ we have $(f, g) \not\approx (f', g')$. Hence, there must exist a state σ such that

$$\begin{aligned} g(\sigma) \neq \infty \quad \text{or} \quad g'(\sigma) \neq \infty \\ \text{and} \quad g(\sigma) \neq g'(\sigma) \quad \text{or} \quad f(\sigma) \neq f'(\sigma). \end{aligned}$$

But if that were the case, then for that state σ either

$$\begin{aligned} \lim_{n \rightarrow \omega} g_n(\sigma) = g(\sigma) \neq g'(\sigma) = \lim_{n \rightarrow \omega} g_n(\sigma), \quad \text{or} \\ \lim_{n \rightarrow \omega} f_n(\sigma) = f(\sigma) \neq f'(\sigma) = \lim_{n \rightarrow \omega} f_n(\sigma) \end{aligned}$$

should hold, both of which is a contradiction to the fact that limits of real numbers are unique if they exist. Therefore, the assumption $\langle f, g \rangle \neq \langle f', g' \rangle$ cannot be true and the limit of $(\langle f_n, g_n \rangle)_{n \in \mathbb{N}}$ must be unique. \square

Due to the limit's uniqueness, we are now in a position to write

$$\lim_{n \rightarrow \omega} \langle f_n, g_n \rangle = \langle f, g \rangle,$$

if a limit exists and $\langle f, g \rangle$ is *the* limit of $\lim_{n \rightarrow \omega} \langle f_n, g_n \rangle$.

Using the limit construct, the $\widetilde{\mathbf{wp}}$ of $\text{while}(\xi)\{C'\}$ is defined as the limit of iteratively applying the characteristic functional of $\text{while}(\xi)\{C'\}$, given by

$$C'F_{\langle f, g \rangle}^{\xi} \langle X, Y \rangle = \llbracket \neg \xi \rrbracket \cdot \langle f, g \rangle + \llbracket \xi \rrbracket \cdot \widetilde{\mathbf{wp}}[C'] \langle X, Y \rangle,$$

to $\langle 0, 0 \rangle$. Formally, we have defined in [Table II](#)

$$\widetilde{\mathbf{wp}}[\text{while}(\xi)\{C'\}] \langle f, g \rangle = \lim_{n \rightarrow \omega} C'F_{\langle f, g \rangle}^n \langle 0, 0 \rangle,$$

where $C'F_{\langle f, g \rangle}^n$ denotes the n -fold application of $C'F_{\langle f, g \rangle}^{\xi}$ to its argument. This is somewhat similar to the \mathbf{wp} -semantics for non-negative expectations, where we basically have $\mathbf{wp}[\text{while}(\xi)\{C'\}](f) = \lim_{n \rightarrow \omega} C'F_f^n(\mathbf{0})$, since the Kleene Fixed Point Theorem gives

$$\begin{aligned} \mathbf{wp}[\text{while}(\xi)\{C'\}](f) &= \text{lfp}_{C'F_f^{\xi}} \\ &= \sup_n C'F_f^n(\mathbf{0}) \quad (\text{Kleene Fixed Point Theorem}) \\ &= \lim_{n \rightarrow \omega} C'F_f^n(\mathbf{0}), \quad \left(C'F_f^n(\mathbf{0}) \text{ increases monot. in } n \right) \end{aligned}$$

and ensures existence of this limit. This, however, works only because $\mathbf{0}$ is the least element in the complete partial order $(\mathbb{E}_{\geq 0}^{\infty}, \leq)$ and because of the monotonicity of $C'F_f^{\xi}$ (which follows from continuity) we automatically obtain an ascending chain $\mathbf{0} \leq C'F_f^{\xi}(\mathbf{0}) \leq C'F_f^2(\mathbf{0}) \leq C'F_f^3(\mathbf{0}) \leq \dots$, for which a supremum exists by completeness of the underlying partial order.

In contrast to that, $\langle 0, 0 \rangle$ is not the least element in the partial order $(\mathbb{IE}, \sqsubseteq)$ and therefore, the sequence

$$\left(C'F_{\langle f, g \rangle}^n \right)_{n \in \mathbb{N}} \langle 0, 0 \rangle$$

is not necessarily an ascending chain. It is because of that, that the Kleene Fixed Point Theorem fails in the context of integrability-witnessing expectations. We have to ensure the existence of the limit defining the semantics of while-loops by other means. Obviously, it is desired that this limit always exists in order for $\widetilde{\mathbf{wp}}$ to be a well-defined semantics for *all possible programs* together with *all possible post-expectations*, and indeed, we can establish the following result:

Theorem 3 (Well-Definedness of $\widetilde{\mathbf{wp}}$ for While-Loops). *Let $\xi \in \text{PGuards}$, $C' \in \text{pProgs}$, and $\langle f, g \rangle \in \mathbb{IE}$. Then the limit*

$$\widetilde{\mathbf{wp}}[\text{while}(\xi)\{C'\}] \langle f, g \rangle = \lim_{n \rightarrow \omega} C'F_{\langle f, g \rangle}^n \langle 0, 0 \rangle$$

exists and hence the $\widetilde{\mathbf{wp}}$ -semantics of any while-loop with respect to any post-expectation is well-defined.

The core idea for proving this theorem is adopted from a well-known proof proving that every absolutely convergent series is also convergent. Let us go over this proof: If a series $S_{a_i} = \sum_{i=0}^{\infty} a_i$ converges absolutely this means that $S_{|a_i|} = \sum_{i=0}^{\infty} |a_i|$ converges to some value a , which implies that it does so unconditionally and monotonically since all summands are positive. This, in turn, implies that $S_{2 \cdot |a_i|} = \sum_{i=0}^{\infty} 2 \cdot |a_i|$ converges unconditionally and monotonically to $2 \cdot a$. Since $0 \leq a_i + |a_i| \leq 2 \cdot |a_i|$ holds, we obtain

$$0 \leq \sum_{i=0}^{\infty} |a_i| + a_i \leq \sum_{i=0}^{\infty} 2 \cdot |a_i| = 2 \cdot a.$$

By that we can see that the series $S_{|a_i|+a_i} = \sum_{i=0}^{\infty} |a_i| + a_i$ is bounded. Furthermore, since $|a_i| + a_i$ must be positive, $S_{|a_i|+a_i}$ is monotonically increasing and therefore $S_{|a_i|+a_i} = \sum_{i=0}^{\infty} |a_i| + a_i$ converges unconditionally. Now, since S_{a_i} is given as the difference of two unconditionally convergent series, namely $S_{a_i} = S_{|a_i|+a_i} - S_{|a_i|}$ the series S_{a_i} must also converge. This basic idea of “express $\sum a_i$ as $\sum |a_i| + a_i - \sum |a_i|$ ” in case that these latter two sums exist, is the underlying principle of the following proof.

Proof of Theorem 3. The idea of this proof is to show by induction on the nesting depth of while-loops and by induction on n that

$$C'F_{\langle f, g \rangle}^n \langle 0, 0 \rangle = \langle C'F_{|f|+f}^n(\mathbf{0}) - C'F_{|f|}^n(\mathbf{0}), C'F_g^n(\mathbf{0}) \rangle$$

holds for all n and any C' . It is then left to show that the limit of the above exists for $n \rightarrow \omega$. We can see that the second component of that sequence increases monotonically towards

$$\sup_{n \in \mathbb{N}} {}^\xi F_g^n(\mathbf{0}) = \mathbf{wp}[\text{while}(\xi) \{C'\}](g) .$$

Then for any state σ for which $\mathbf{wp}[\text{while}(\xi) \{C'\}](g)(\sigma) < \infty$ holds, we have

$$\begin{aligned} & \sup_{n \in \mathbb{N}} {}^\xi F_{|f|+f}^n(\mathbf{0})(\sigma) \\ &= \mathbf{wp}[\text{while}(\xi) \{C'\}](|f|+f)(\sigma) \\ &\leq \mathbf{wp}[\text{while}(\xi) \{C'\}](2 \cdot |f|)(\sigma) \quad (\mathbf{wp} \text{ monotonic}) \\ &\leq \mathbf{wp}[\text{while}(\xi) \{C'\}](2 \cdot g)(\sigma) \quad (\mathbf{wp} \text{ monotonic}) \\ &\leq 2 \cdot \mathbf{wp}[\text{while}(\xi) \{C'\}](g)(\sigma) \quad (\mathbf{wp} \text{ linear}) \\ &< 2 \cdot \infty = \infty, \text{ and} \end{aligned}$$

$$\begin{aligned} & \sup_{n \in \mathbb{N}} {}^\xi F_{|f|}^n(\mathbf{0})(\sigma) \\ &= \mathbf{wp}[\text{while}(\xi) \{C'\}](|f|)(\sigma) \\ &\leq \mathbf{wp}[\text{while}(\xi) \{C'\}](g)(\sigma) \quad (\mathbf{wp} \text{ monotonic}) \\ &< \infty . \end{aligned}$$

Hence, the limit for both ${}^\xi F_{|f|+f}^n(\mathbf{0})(\sigma)$ and ${}^\xi F_{|f|}^n(\mathbf{0})(\sigma)$ exists, thus also the limit for ${}^\xi F_{|f|+f}^n(\mathbf{0})(\sigma) - {}^\xi F_{|f|}^n(\mathbf{0})(\sigma)$ exists, and therefore $\lim_{n \rightarrow \omega} {}^\xi F_{|f|+f}^n(\mathbf{0})(\sigma) - {}^\xi F_{|f|}^n(\mathbf{0})(\sigma)$ exists, too. \square

Let us revisit the two examples we presented in Section IV-A, i.e. the program

$$C_{geo}: \quad x := 1; \text{ while}(1/2)\{x := x + 1\} ,$$

together with post-expectations $f = 2^x$ and $f' = (-2)^x$, respectively. In the $\widetilde{\mathbf{wp}}$ calculus, the respective pre-expectations are well-defined, namely

$$\begin{aligned} \widetilde{\mathbf{wp}}[C_{geo}]\{2^x, |2^x|\} &= \{ \mathbf{0}, \infty \} \\ \text{and} \quad \widetilde{\mathbf{wp}}[C_{geo}]\{(-2)^x, |(-2)^x|\} &= \{ \mathbf{0}, \infty \} . \end{aligned}$$

So the pre-expectations of these two examples are perfectly well-defined and therefore these examples are not at all pathological in our presented calculus.

VI. PROPERTIES OF THE $\widetilde{\mathbf{wp}}$ -TRANSFORMER

A. Monotonicity

Perhaps the single most important property of the $\widetilde{\mathbf{wp}}$ -transformer is monotonicity, as that is what enables compositional reasoning. Monotonicity is as vital to our calculus as the consequence rule is to Hoare logic. For instance, it enables to continue reasoning soundly using over-approximations obtained by invariant rules. Our transformer enjoys this property:

Theorem 4 (Monotonicity of $\widetilde{\mathbf{wp}}$). *$\widetilde{\mathbf{wp}}$ is monotonic with respect to \sqsubseteq , i.e. for all $C \in \mathbf{pProgs}$ and $\{f, g\}, \{f', g'\} \in \mathbb{IE}$,*

$$\begin{aligned} \{f, g\} &\sqsubseteq \{f', g'\} \\ \text{implies} \quad \widetilde{\mathbf{wp}}[C]\{f, g\} &\sqsubseteq \widetilde{\mathbf{wp}}[C]\{f', g'\} . \end{aligned}$$

Proof. The proof goes by induction on the structure of C . Let $\{f, g\} \sqsubseteq \{f', g'\}$. All cases are straightforward, except for the while-loop. For that, reconsider

$${}^\xi F_{|f|+f}^n(\mathbf{0}, \mathbf{0}) = \left({}^\xi F_{|f|+f}^n(\mathbf{0}) - {}^\xi F_{|f|}^n(\mathbf{0}), {}^\xi F_g^n(\mathbf{0}) \right)$$

from the proof of Theorem 3. Given that fact, the proof boils down to showing by induction on n that the inequality

$$\begin{aligned} & {}^\xi F_{|f|+f}^n(\mathbf{0})(\sigma) - {}^\xi F_{|f|}^n(\mathbf{0})(\sigma) \\ &\leq {}^\xi F_{|f'|+f'}^n(\mathbf{0})(\sigma) - {}^\xi F_{|f'|}^n(\mathbf{0})(\sigma) , \end{aligned} \quad (\dagger)$$

holds if $\mathbf{wp}[\text{while}(\xi) \{C'\}](g')(\sigma) < \infty$ (and therefore by monotonicity also $\mathbf{wp}[\text{while}(\xi) \{C'\}](g)(\sigma) < \infty$) holds. In that case, both

$${}^\xi F_{|f|}^{n+1}(\mathbf{0})(\sigma) \leq {}^\xi F_g^{n+1}(\mathbf{0})(\sigma) \leq \left(\text{lfp}_{C'} {}^\xi F_g \right)(\sigma) < \infty$$

and

$${}^\xi F_{|f'|}^{n+1}(\mathbf{0})(\sigma) \leq {}^\xi F_{g'}^{n+1}(\mathbf{0})(\sigma) \leq \left(\text{lfp}_{C'} {}^\xi F_{g'} \right)(\sigma) < \infty$$

holds, and we can thus rewrite inequality (\dagger) as

$$\begin{aligned} & {}^\xi F_{|f|+f}^n(\mathbf{0})(\sigma) + {}^\xi F_{|f'|}^n(\mathbf{0})(\sigma) \\ &\leq {}^\xi F_{|f'|+f'}^n(\mathbf{0})(\sigma) + {}^\xi F_{|f|}^n(\mathbf{0})(\sigma) , \end{aligned}$$

and prove that statement by induction on n instead. For the induction step, consider the following:

$$\begin{aligned} & {}^\xi F_{|f|+f}^{n+1}(\mathbf{0})(\sigma) + {}^\xi F_{|f'|}^{n+1}(\mathbf{0})(\sigma) \\ &\leq {}^\xi F_{|f'|+f'}^{n+1}(\mathbf{0})(\sigma) + {}^\xi F_{|f|}^{n+1}(\mathbf{0})(\sigma) \end{aligned}$$

iff

$$\begin{aligned} & \left(\llbracket \xi : \text{false} \rrbracket \cdot (|f| + f + |f'|) \right)(\sigma) \\ &+ \left(\llbracket \xi : \text{true} \rrbracket \cdot \mathbf{wp}[C'] \left({}^\xi F_{|f|+f}^n(\mathbf{0}) + {}^\xi F_{|f'|}^n(\mathbf{0}) \right) \right)(\sigma) \\ &\leq \left(\llbracket \xi : \text{false} \rrbracket \cdot (|f'| + f' + |f|) \right)(\sigma) \\ &+ \left(\llbracket \xi : \text{true} \rrbracket \cdot \mathbf{wp}[C'] \left({}^\xi F_{|f'|+f'}^n(\mathbf{0}) + {}^\xi F_{|f|}^n(\mathbf{0}) \right) \right)(\sigma) , \end{aligned}$$

(by definition of characteristic functional and linearity of \mathbf{wp})

which follows from the induction hypothesis on n and by monotonicity of \mathbf{wp} . \square

B. Reasoning about Loops

Whereas reasoning about non-loopy programs is mostly straightforward, reasoning about the $\widetilde{\mathbf{wp}}$ of a loop is more complicated as it involves reasoning about limits of integrability-witnessing expectation sequences. To help overcoming this difficulty, we present now an invariant-based approach that allows for over-approximating those limits.

We have already seen that the fact

$${}^\xi F_{|f|+f}^n(\mathbf{0}, \mathbf{0}) = \left({}^\xi F_{|f|+f}^n(\mathbf{0}) - {}^\xi F_{|f|}^n(\mathbf{0}), {}^\xi F_g^n(\mathbf{0}) \right)$$

from the proof of Theorem 3 was vital to showing monotonicity of the $\widetilde{\mathbf{wp}}$ -transformer. It will also allow us to reason about integrability-witnessing pre-expectations through reasoning

about standard weakest pre-expectations, which is simpler since we have an easy-to-apply invariant rule for these.

If we take a closer look at the sequence

$$\left(\int_{C' F_{|f|+f}^n(\mathbf{0})}^{\xi F_g^n(\mathbf{0})}, \int_{C' F_g^n(\mathbf{0})}^{\xi F_{|f|+f}^n(\mathbf{0})} \right)_{n \in \mathbb{N}}$$

we can see that in order to over-approximate the limit of that sequence, we can—simply put—

- 1) over-approximate the limit—i.e. the supremum—of $\int_{C' F_g^n(\mathbf{0})}^{\xi F_g^n(\mathbf{0})}$,
- 2) over-approximate the limit—i.e. again the supremum—of $\int_{C' F_{|f|+f}^n(\mathbf{0})}^{\xi F_{|f|+f}^n(\mathbf{0})}$, and
- 3) under-approximate the limit—once again: the supremum—of $\int_{C' F_{|f|}^n(\mathbf{0})}^{\xi F_{|f|}^n(\mathbf{0})}$.

Notice that these over- and under-approximations are over- and under-approximations of standard weakest pre-expectations. Furthermore, recall that by Theorem 1 (4) and (5) we have invariant rules for those over- and under-approximations. This immediately leads us to the following proof rule for loops:

Theorem 5 (Loop Invariants for $\widetilde{\text{wp}}$). *Let $\{f, g\} \in \mathbb{IE}$, $C' \in \text{pProgs}$, $I, G \in \mathbb{E}_{\geq 0}^\infty$ with $G(\sigma) < \infty$, for all $\sigma \in \Sigma$, and $(H_n)_{n \in \mathbb{N}} \subseteq \mathbb{E}_{\geq 0}^\infty$. Then $\int_{C' F_g^n(\mathbf{0})}^{\xi F_g^n(\mathbf{0})} \leq G$, $\int_{C' F_{|f|+f}^n(\mathbf{0})}^{\xi F_{|f|+f}^n(\mathbf{0})} \leq I$, $H_0 \leq \int_{C' F_{|f|}^n(\mathbf{0})}^{\xi F_{|f|}^n(\mathbf{0})}$, and $H_{n+1} \leq \int_{C' F_{|f|}^n(H_n)}^{\xi F_{|f|}^n(H_n)}$ implies*

$$\widetilde{\text{wp}}[\text{while}(\xi)\{C'\}]\{f, g\} \sqsubseteq \int I - \sup_{n \in \mathbb{N}} H_n, 2 \cdot G \int.$$

By similar considerations, we can find a dual theorem for lower bounds, see Appendix C. Notice that we have to use $2 \cdot G$ in the second component of the over-approximation of $\widetilde{\text{wp}}[\text{while}(\xi)\{C'\}]\{f, g\}$. This is just to ensure that the second component really bounds the absolute value of the first component. Using G instead might not yield a proper member of \mathbb{IE} . Notice that using $2 \cdot G$ does not effect the integrability-witnessing property of the second component.

Let us now illustrate the use of the loop invariant rule from Theorem 5 by means of a worked example:

Example 4 (Towards Amortized Expected Run-Time Analysis). Suppose we need to perform an amortized analysis of a randomized data structure by means of a potential function Φ . Suppose further that a certain operation Op first increases the potential by 1 and thereafter keeps flipping a coin until the first heads. With every flip of tails though, the potential is decreased by 3. We can model this situation by means of the following probabilistic program:

$$C_{Op}: \quad \Phi := \Phi + 1; \text{while } (1/2) \{ \Phi := \Phi - 3 \}$$

Here Φ represents the change in the potential function Φ . Notice that the change in potential might very well be positive (in fact with probability $1/2$) as well as negative, so both possibilities have to be accounted for.

Even though an application of the operation Op might increase the potential, we now want to prove that an application of Op decreases the potential *in expectation*. This amounts

to proving that the pre-expectation of Φ evaluated in any initial state σ with $\sigma(\Phi) = 0$ is negative. For that, we need to calculate

$$\begin{aligned} \widetilde{\text{wp}}[C_{Op}]\{\Phi, |\Phi|\} &= \widetilde{\text{wp}}[\Phi := \Phi + 1; \text{while } (1/2) \{ \dots \}]\{\Phi, |\Phi|\} \\ &= \widetilde{\text{wp}}[\Phi := \Phi + 1](\widetilde{\text{wp}}[\text{while } (1/2) \{ \dots \}]\{\Phi, |\Phi|\}) \end{aligned}$$

So the first thing we need to do is to reason about the pre-expectation of the while-loop. Appealing to Theorem 5, we propose following loop invariants

$$G = \sum_{i=0}^{\omega} \frac{|\Phi - 3 \cdot i|}{2^{i+1}}, \quad I = \sum_{i=0}^{\omega} \frac{|\Phi - 3 \cdot i|}{2^{i+1}} + \Phi - 3,$$

and $H_n = \sum_{i=0}^n \frac{|\Phi - 3 \cdot i|}{2^{i+1}}.$

Indeed, one can verify that these loop invariants satisfy the preconditions of Theorem 5. Furthermore, we observe that $\sup_{n \in \mathbb{N}} H_n = G$ holds. Applying Theorem 5 therefore yields

$$\widetilde{\text{wp}}[\text{while } (1/2) \{ \Phi := \Phi - 3 \}]\{\Phi, |\Phi|\} \sqsubseteq \int I - G, 2 \cdot G \int.$$

Because G and I are absolutely convergent for any valuation of Φ (e.g. by the ratio test), we can calculate $I - G = \Phi - 3$, and so we get

$$\widetilde{\text{wp}}[\text{while } (1/2) \{ \Phi := \Phi - 3 \}]\{\Phi, |\Phi|\} \sqsubseteq \int \Phi - 3, 2 \cdot G \int.$$

Since $\widetilde{\text{wp}}$ is monotonic (see Theorem 4), we can now safely continue our reasoning with the over-approximation $\int \Phi - 3, 2 \cdot G \int$ and calculate

$$\widetilde{\text{wp}}[\Phi := \Phi + 1]\int \Phi - 3, 2G \int = \int \Phi - 2, \sum_{i=0}^{\omega} \frac{|\Phi + 1 - 3i|}{2^{i+1}} \int.$$

By that, we get in total an over-approximation of the sought-after pre-expectation $\widetilde{\text{wp}}[C_{Op}]\{\Phi, |\Phi|\}$. If we instantiate the second component of that over-approximation in an initial state σ with $\sigma(\Phi) = 0$, we get

$$\sum_{i=0}^{\omega} \frac{|0 + 1 - 3 \cdot i|}{2^{i+1}} = 3 < \infty.$$

So the expected value at σ was integrable and thus it makes sense to evaluate the first component in σ (which is what we are really interested in). This gives $0 - 2 = -2$ and thus executing Op decreases the potential *in expectation* by 2. \triangle

Notice that the analysis performed as in Example 4 would not be possible using either the deduction rules of PPD \mathcal{L} [4] or the invariant-based approach of McIver & Morgan's wp -calculus [3] off-the-shelf. Instead, a tailor-made argument would be needed for reasoning about the mixed-sign Φ . For more details on this matter and a more involved worked example, see Appendix B.

C. Soundness

The last but certainly not least important property that we establish for our $\widetilde{\text{wp}}$ transformer is that it is sound, meaning that if we can establish $\widetilde{\text{wp}}[C]\{f, g\} = \{f', g'\}$ then $f'(\sigma)$ is in fact the expected value of f after termination of C on initial state σ . For that, we first generalize the fact established in the proof of Theorem 3:

Lemma 1. *Let $\{f, g\} \in \mathbb{IE}$ with $\text{wp}[C](g)(\sigma) < \infty$ and $\{f', g'\} = \widetilde{\text{wp}}[C]\{f, g\}$. Then $f'(\sigma) = \text{wp}[C](|f| + f)(\sigma) - \text{wp}[C](|f|)(\sigma)$.*

Proof. By induction on C using the fact from the proof of Theorem 3. \square

In standard probability theory any mixed-sign random variable f can be decomposed into a positive part $+f = \lambda\sigma \bullet \max\{0, f(\sigma)\} \in \mathbb{E}_{\geq 0}^\infty$ and a negative part $-f = \lambda\sigma \bullet -\min\{0, f(\sigma)\} \in \mathbb{E}_{\geq 0}^\infty$, with $f = +f - f$. Notice that $+f$ and $-f$ are both non-negative expectations. The expected value of f is then defined as the expected value of $+f$ minus the expected value of $-f$, i.e. as

$$\mathbb{E}_\mu(f) = \mathbb{E}_\mu(+f) - \mathbb{E}_\mu(-f),$$

if both $\mathbb{E}_\mu(+f) < \infty$ and $\mathbb{E}_\mu(-f) < \infty$. Using this—sometimes called—*Jordan decomposition* of f , we can now establish the following lemma:

Lemma 2. *Let $f \in \mathbb{E}^*$, $g \in \mathbb{E}_{\geq 0}^\infty$ with $|f| \leq g$, $\text{wp}[C](g)(\sigma) < \infty$, $\widetilde{\text{wp}}[C]\{f, g\} = \{f', g'\}$, and $f = +f - f$. Then $f'(\sigma) + \text{wp}[C](-f)(\sigma) = \text{wp}[C](+f)(\sigma)$.*

Proof. Consider the following:

$$\begin{aligned} f'(\sigma) + \text{wp}[C](-f)(\sigma) &= \text{wp}[C](+f)(\sigma) \\ \iff \text{wp}[C](|f| + f)(\sigma) - \text{wp}[C](|f|)(\sigma) + \text{wp}[C](-f)(\sigma) & \\ &= \text{wp}[C](+f)(\sigma) \quad (\text{Lemma 1}) \\ \iff \text{wp}[C](|f| + f)(\sigma) + \text{wp}[C](-f)(\sigma) & \\ &= \text{wp}[C](+f)(\sigma) + \text{wp}[C](|f|)(\sigma) \\ &\quad (\text{by } \text{wp}[C](|f|)(\sigma) \leq \text{wp}[C](g)(\sigma) < \infty) \\ \iff \text{wp}[C](|f| + f + -f)(\sigma) = \text{wp}[C](+f + |f|)(\sigma) & \\ &\quad (\text{by linearity of } \text{wp}) \\ \iff \text{wp}[C](|f| + +f)(\sigma) = \text{wp}[C](+f + |f|)(\sigma) & \\ &\quad (\text{by } f = +f - f \text{ iff } +f = f + -f) \\ \iff \text{true} \quad \square \end{aligned}$$

The soundness of the $\widetilde{\text{wp}}$ transformer follows now almost immediately from Lemma 2.

Theorem 6 (Soundness of $\widetilde{\text{wp}}$). *Let $f \in \mathbb{E}^*$, $\text{wp}[C](|f|)(\sigma) < \infty$, and let $\widetilde{\text{wp}}[C]\{f, |f|\} = \{f', g'\}$. Then $f'(\sigma)$ is the expected value of f after termination of program C on state σ , i.e. if $f = +f - f$, then*

$$f'(\sigma) = \text{wp}[C](+f)(\sigma) - \text{wp}[C](-f)(\sigma).$$

Proof. In principle by setting $g = |f|$ in Lemma 2. \square

VII. CONCLUSION

We have presented a sound weakest pre-expectation calculus for reasoning about *mixed-sign unbounded* expectations. With this calculus, a pre-expectation can always be obtained, even in those cases where classical pre-expectations (i.e. expected values) do not exist. We have shown that the semantics of while-loops is always well-defined in terms of a limit of iteratively applying a functional to a zero-element despite the fact that a standard least fixed point argument is not applicable in this context. For reasoning about loops, we have presented an invariant-based technique and we have shown its applicability to an example inspired by amortized analysis of randomized algorithms.

ACKNOWLEDGEMENTS

We would like to thank the anonymous referees on their constructive feedback on an earlier version of this paper.

REFERENCES

- [1] A. D. Gordon, T. A. Henzinger, A. V. Nori, and S. K. Rajamani, “Probabilistic Programming,” in *Future of Software Engineering (FOSE)*. ACM, 2014, pp. 167–181.
- [2] E. W. Dijkstra, *A Discipline of Programming*. Prentice Hall, 1976.
- [3] A. McIver and C. Morgan, *Abstraction, Refinement and Proof for Probabilistic Systems*. Springer, 2004.
- [4] D. Kozen, “A probabilistic PDL,” *J. Comput. Syst. Sci.*, vol. 30, no. 2, pp. 162–178, 1985.
- [5] C. Jones, “Probabilistic non-determinism,” Ph.D. dissertation, University of Edinburgh. College of Science and Engineering. School of Informatics., 1990.
- [6] E. C. R. Hehner, “A Probability Perspective,” *Formal Aspects of Computing*, vol. 23, no. 4, pp. 391–419, 2011.
- [7] B. L. Kaminski, J. Katoen, C. Matheja, and F. Olmedo, “Weakest Precondition Reasoning for Expected Run-Times of Probabilistic Programs,” in *ESOP*, ser. LNCS, vol. 9632. Springer, 2016, pp. 364–389.
- [8] F. Olmedo, B. L. Kaminski, J. Katoen, and C. Matheja, “Reasoning about Recursive Probabilistic Programs,” in *LICS*. ACM/IEEE, 2016, pp. 672–681.
- [9] A. McIver and C. Morgan, “Partial Correctness for Probabilistic Demon Programs,” *Theor. Comput. Sci.*, vol. 266, no. 1–2, pp. 513–541, 2001.
- [10] J. Hurd, “A Formal Approach to Probabilistic Termination,” in *Theorem Proving in Higher Order Logics (TPHOL)*, ser. LNCS. Springer Berlin Heidelberg, 2002, vol. 2410, pp. 230–245.
- [11] D. Cock, “pGCL for Isabelle,” *Archive of Formal Proofs*, 2014. [Online]. Available: <http://afp.sourceforge.net/entries/pGCL.shtml>
- [12] J. Hölzl, “Formalising Semantics for Expected Running Time of Probabilistic Programs,” in *Interactive Theorem Proving (ITP)*, ser. LNCS, vol. 9807. Springer, 2016, pp. 475–482.
- [13] S. Albers and M. Karpinski, “Randomized Splay Trees: Theoretical and Experimental Results,” *Information Processing Letters*, vol. 81, no. 4, pp. 213–221, 2002.
- [14] A. Chakarov and S. Sankaranarayanan, “Probabilistic Program Analysis with Martingales,” in *Computer Aided Verification (CAV)*, ser. LNCS, vol. 8044. Springer Berlin Heidelberg, 2013, pp. 511–526.
- [15] F. Gretz, J. Katoen, and A. McIver, “Operational versus Weakest Pre-Expectation Semantics for the Probabilistic Guarded Command Language,” *Performance Evaluation*, vol. 73, pp. 110–132, 2014.
- [16] G. Winskel, *The Formal Semantics of Programming Languages: An Introduction*. MIT Press, 1993.
- [17] J.-L. Lassez, V. Nguyen, and E. Sonenberg, “Fixed Point Theorems and Semantics: A Folk Tale,” *Information Processing Letters*, vol. 14, no. 3, pp. 112–116, 1982.
- [18] S. Abramsky and A. Jung, “Domain Theory,” in *Handbook of Logic in Computer Science (Vol. 3)*. Oxford University Press, 1994, pp. 1–168.
- [19] B. Riemann, *Ueber die Darstellbarkeit einer Function durch eine trigonometrische Reihe*. Königliche Gesellschaft der Wissenschaften zu Göttingen, 1867.

APPENDIX

A. Proof of Expected Run-Time for Kozen's Example

The example studied by Kozen [4] is given by the following program:

```

x := n; c := 0;
while (x ≠ 0) {
  if (1/2) {skip} else {x := x - 1};
  c := c + 1}

```

As [4], we assume that all program variables range over the integers and that $n > 0$. The (asymptotic) expected run-time of this program is given by the expected value of c after termination of the program, as c counts the number of loop iterations. A detailed proof that $2n$ is an upper bound of that expected run-time carried out in the **wp**-calculus is given in the following:

Proof. We start our analysis with post-expectation c . Appealing to Theorem 1 (4), we look for an upper invariant I for the while-loop, such that

$$\llbracket x = 0 \rrbracket \cdot c + \llbracket x \neq 0 \rrbracket \cdot \mathbf{wp}[body](I) \leq I, \quad (2)$$

e.g. $I = \llbracket x \geq 0 \rrbracket (c + 2x)$. Next, we check that I indeed satisfies Equation (2):

$$\begin{aligned}
& \llbracket x = 0 \rrbracket \cdot c + \llbracket x \neq 0 \rrbracket \cdot \mathbf{wp}[body](I) \\
&= \llbracket x = 0 \rrbracket \cdot c + \llbracket x \neq 0 \rrbracket \cdot \mathbf{wp}[\text{if } (1/2) \{ \dots \}; c := c + 1](I) \\
&= \llbracket x = 0 \rrbracket \cdot c + \llbracket x \neq 0 \rrbracket \cdot \mathbf{wp}[\text{if } \dots](\llbracket x \geq 0 \rrbracket (c + 1 + 2x)) \\
&= \llbracket x = 0 \rrbracket \cdot c + \llbracket x \neq 0 \rrbracket \cdot \frac{1}{2} (\llbracket x \geq 0 \rrbracket (c + 1 + 2x) \\
&\quad + \llbracket x - 1 \geq 0 \rrbracket (c + 1 + 2(x - 1))) \\
&= \llbracket x = 0 \rrbracket \cdot c \\
&\quad + \frac{1}{2} (\llbracket x \geq 1 \rrbracket (c + 1 + 2x) + \llbracket x \geq 1 \rrbracket (c + 1 + 2(x - 1))) \\
&= \llbracket x = 0 \rrbracket \cdot c + \frac{1}{2} \llbracket x \geq 1 \rrbracket (c + 1 + 2x + c + 1 + 2(x - 1)) \\
&= \llbracket x = 0 \rrbracket \cdot (c + 2x) + \llbracket x \geq 1 \rrbracket (c + 2x) \\
&= \llbracket x \geq 0 \rrbracket (c + 2x) = I \leq I
\end{aligned}$$

By Theorem 1 (4) we have now established

$$\mathbf{wp}[\text{while}(x \neq 0) \{ body \}](c) \leq \llbracket x \geq 0 \rrbracket (c + 2x),$$

and by monotonicity of **wp**, we can proceed our analysis with

$$\begin{aligned}
& \mathbf{wp}[x := n; c := 0](I) \\
&= \mathbf{wp}[x := n](\llbracket x \geq 0 \rrbracket (0 + 2x)) = \llbracket n \geq 0 \rrbracket \cdot 2n.
\end{aligned}$$

By assumption $n > 0$, we have proven the run-time bound $2n$. \square

All calculations in the invariant verification involved only basic arithmetic. The **wp**-style proof that $2n$ is also a

lower bound is slightly more involved. The reader is invited to compare the above reasoning to the reasoning using PDDL [4, pages 176–177].

B. A More Involved Example

Consider the following program

```
while (1/2) {x := -x - sign(x)}
```

We are interested in the expected value of program variable x and will establish upper bounds for this expected value by means of two methods: first using the approach present in this paper and second by a Jordan-decomposition-based approach. We will see that the latter is more involved.

1) *Analysis Using Integrability-Witnessing Expectations:* We perform an analysis of

$$\widetilde{\mathbf{wp}}[\text{while}(1/2) \{ C' \}](x, |x|),$$

where we denote by C' the program $x := -x - \text{sign}(x)$ for the sake of readability. Appealing to Theorem 5, we propose the following loop invariants:

$$\begin{aligned}
G &= |x| + 1, \quad I = |x| + \llbracket x \neq 0 \rrbracket + \frac{x}{3} - \frac{\text{sign}(x)}{9}, \\
\text{and} \quad H_n &= \sum_{i=0}^n \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot i}{2^{i+1}}
\end{aligned}$$

Next, we need to verify the four preconditions of Theorem 5. First, ${}^{1/2}_{C'}F_{|x|}(G) \leq G$:

$$\begin{aligned}
{}^{1/2}_{C'}F_{|x|}(G) &= \frac{1}{2} \cdot |x| + \frac{1}{2} \cdot \mathbf{wp}[C'](|x| + 1) \\
&= \frac{|x|}{2} + \frac{1}{2} \cdot (|-x - \text{sign}(x)| + 1) \\
&= \frac{|x|}{2} + \frac{|x| + \llbracket x \neq 0 \rrbracket + 1}{2} \\
&\leq \frac{|x|}{2} + \frac{|x| + 1 + 1}{2} \\
&= |x| + 1 = G
\end{aligned}$$

Second, ${}^{1/2}_{C'}F_{|x|+x}(I) \leq I$:

$$\begin{aligned}
& {}^{1/2}_{C'}F_{|x|+x}(I) \\
&= \frac{1}{2} \cdot (|x| + x) \\
&\quad + \frac{1}{2} \cdot \mathbf{wp}[C'] \left(|x| + \llbracket x \neq 0 \rrbracket + \frac{x}{3} - \frac{\text{sign}(x)}{9} \right) \\
&= \frac{|x| + x}{2} + \frac{1}{2} \left(|-x - \text{sign}(x)| + \llbracket -x - \text{sign}(x) \neq 0 \rrbracket \right. \\
&\quad \left. + \frac{-x - \text{sign}(x)}{3} - \frac{\text{sign}(-x - \text{sign}(x))}{9} \right) \\
&= \frac{|x| + x}{2} + \frac{|x| + \llbracket x \neq 0 \rrbracket + \llbracket x \neq 0 \rrbracket}{2} \\
&\quad + \frac{-x - \text{sign}(x)}{6} + \frac{\text{sign}(x)}{18} \\
&= |x| + \llbracket x \neq 0 \rrbracket + \frac{x}{3} - \frac{\text{sign}(x)}{9} = I \leq I
\end{aligned}$$

Third, $\frac{1}{2}F_{|x|}(\mathbf{0}) \geq H_0$:

$$\begin{aligned}
\frac{1}{2}F_{|x|}(\mathbf{0}) &= \frac{1}{2} \cdot |x| + \frac{1}{2} \cdot \mathbf{wp}[C'](\mathbf{0}) \\
&= \frac{|x|}{2} + \frac{1}{2} \cdot \mathbf{0} \\
&= \frac{|x|}{2} \\
&= \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot 0}{2^{0+1}} \\
&= \sum_{i=0}^0 \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot i}{2^{i+1}} = H_0 \geq H_0
\end{aligned}$$

Fourth, $\frac{1}{2}F_{|x|}(H_n) \geq H_{n+1}$:

$$\begin{aligned}
\frac{1}{2}F_{|x|}(H_n) &= \frac{1}{2} \cdot |x| + \frac{1}{2} \cdot \mathbf{wp}[C'] \left(\sum_{i=0}^n \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot i}{2^{i+1}} \right) \\
&= \frac{|x|}{2} + \frac{1}{2} \left(\sum_{i=0}^n \frac{|-x - \mathbf{sign}(x)| + \llbracket -x - \mathbf{sign}(x) \neq 0 \rrbracket \cdot i}{2^{i+1}} \right) \\
&= \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot 0}{2^{0+1}} + \sum_{i=0}^n \frac{|x| + \llbracket x \neq 0 \rrbracket + \llbracket x \neq 0 \rrbracket \cdot i}{2^{i+1+1}} \\
&= \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot 0}{2^{0+1}} + \sum_{i=0}^n \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot (i+1)}{2^{i+1+1}} \\
&= \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot 0}{2^{0+1}} + \sum_{i=1}^{n+1} \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot i}{2^{i+1}} \\
&= \sum_{i=0}^{n+1} \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot i}{2^{i+1}} = H_{n+1} \geq H_{n+1}
\end{aligned}$$

Finally, we have to analyze $\sup_{n \in \mathbb{N}} H_n$, which is fairly straightforward:

$$\begin{aligned}
\sup_{n \in \mathbb{N}} H_n &= \sup_{n \in \mathbb{N}} \sum_{i=0}^n \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot i}{2^{i+1}} \\
&= \sum_{i=0}^{\omega} \frac{|x| + \llbracket x \neq 0 \rrbracket \cdot i}{2^{i+1}} \\
&= |x| \cdot \sum_{i=0}^{\omega} \frac{1}{2^{i+1}} + \llbracket x \neq 0 \rrbracket \cdot \sum_{i=0}^{\omega} \frac{i}{2^{i+1}} \\
&= |x| \cdot 1 + \llbracket x \neq 0 \rrbracket \cdot 1 \\
&= |x| + \llbracket x \neq 0 \rrbracket
\end{aligned}$$

Applying Theorem 5 therefore yields

$$\begin{aligned}
&\widetilde{\mathbf{wp}}[\text{while}(1/2)\{C'\}]\{x, |x|\} \\
&\sqsubseteq \left\langle I - \sup_{n \in \mathbb{N}} H_n, 2 \cdot G \right\rangle \\
&= \left\langle \frac{x}{3} - \frac{\mathbf{sign}(x)}{9}, 2 \cdot G \right\rangle
\end{aligned}$$

Since $2|x| + 2 < \infty$, we obtain that $x/3 - \mathbf{sign}(x)/9$ is an over-approximation of the expected value of x after execution of the program for any initial state.

2) *Analysis Using Jordan Decomposition:* If one wanted to perform an equivalent analysis using the Jordan decomposition of x into $^+x = \max\{x, 0\}$ and $^-x = -\min\{x, 0\}$, one would have to first prove integrability of ^+x and ^-x . For that, it suffices to find two invariants G_{+x} and G_{-x} such that both $\frac{1}{2}F_{+x}(G_{+x}) \leq G_{+x}$ and $\frac{1}{2}F_{-x}(G_{-x}) \leq G_{-x}$. The simplest invariants we were able to come up with are:

$$\begin{aligned}
G_{+x} &= \llbracket x > 0 \rrbracket \cdot \left(\frac{2}{3}x + \frac{4}{9} \right) + \llbracket x < 0 \rrbracket \cdot \left(-\frac{1}{3}x + \frac{5}{9} \right) \\
G_{-x} &= \llbracket x > 0 \rrbracket \cdot \left(\frac{1}{3}x + \frac{5}{9} \right) + \llbracket x < 0 \rrbracket \cdot \left(-\frac{2}{3}x + \frac{4}{9} \right)
\end{aligned}$$

Next, we have to establish that those are indeed invariants.

First, $\frac{1}{2}F_{+x}(G_{+x}) \leq G_{+x}$:

$$\begin{aligned}
\frac{1}{2}F_{+x}(G_{+x}) &= \frac{1}{2} \cdot ^+x + \frac{1}{2} \cdot \mathbf{wp}[C'] \left(\llbracket x > 0 \rrbracket \cdot \left(\frac{2}{3}x + \frac{4}{9} \right) \right. \\
&\quad \left. + \llbracket x < 0 \rrbracket \cdot \left(-\frac{1}{3}x + \frac{5}{9} \right) \right) \\
&= \frac{1}{2} \cdot ^+x \\
&\quad + \frac{1}{2} \cdot \left(\llbracket -x - \mathbf{sign}(x) > 0 \rrbracket \cdot \left(\frac{2}{3}(-x - \mathbf{sign}(x)) + \frac{4}{9} \right) \right. \\
&\quad \left. + \llbracket -x - \mathbf{sign}(x) < 0 \rrbracket \cdot \left(-\frac{1}{3}(-x - \mathbf{sign}(x)) + \frac{5}{9} \right) \right) \\
&= \frac{1}{2} \llbracket x > 0 \rrbracket x + \frac{1}{2} \cdot \left(\llbracket x < 0 \rrbracket \cdot \left(\frac{2}{3}(-x + 1) + \frac{4}{9} \right) \right. \\
&\quad \left. + \llbracket x > 0 \rrbracket \cdot \left(-\frac{1}{3}(-x - 1) + \frac{5}{9} \right) \right) \\
&= \llbracket x > 0 \rrbracket \left(\frac{1}{2}x - \frac{1}{3}(-x - 1) + \frac{5}{9} \right) \\
&\quad + \llbracket x < 0 \rrbracket \cdot \left(\frac{1}{2} \cdot \left(\frac{2}{3}(-x + 1) + \frac{4}{9} \right) \right) \\
&= \llbracket x > 0 \rrbracket \cdot \left(\frac{2}{3}x + \frac{4}{9} \right) + \llbracket x < 0 \rrbracket \cdot \left(-\frac{1}{3}x + \frac{5}{9} \right) \\
&= G_{+x} \leq G_{+x}
\end{aligned}$$

Second, $\frac{1}{2}F_{-x}(G_{-x}) \leq G_{-x}$:

$$\begin{aligned}
\frac{1}{2}F_{-x}(G_{-x}) &= \frac{1}{2} \cdot ^-x + \frac{1}{2} \cdot \mathbf{wp}[C'] \left(\llbracket x > 0 \rrbracket \cdot \left(\frac{1}{3}x + \frac{5}{9} \right) \right. \\
&\quad \left. + \llbracket x < 0 \rrbracket \cdot \left(-\frac{2}{3}x + \frac{4}{9} \right) \right) \\
&= \frac{1}{2} \cdot ^-x \\
&\quad + \frac{1}{2} \cdot \left(\llbracket -x - \mathbf{sign}(x) > 0 \rrbracket \cdot \left(\frac{1}{3}(-x - \mathbf{sign}(x)) + \frac{5}{9} \right) \right. \\
&\quad \left. + \llbracket -x - \mathbf{sign}(x) < 0 \rrbracket \cdot \left(-\frac{2}{3}(-x - \mathbf{sign}(x)) + \frac{4}{9} \right) \right) \\
&= \frac{1}{2} \llbracket x > 0 \rrbracket x + \frac{1}{2} \cdot \left(\llbracket x < 0 \rrbracket \cdot \left(\frac{1}{3}(-x + 1) + \frac{5}{9} \right) \right.
\end{aligned}$$

$$\begin{aligned}
& + \llbracket x > 0 \rrbracket \cdot \left(-\frac{2}{3}(-x-1) + \frac{4}{9} \right) \\
& = \llbracket x > 0 \rrbracket \left(\frac{1}{2}x - \frac{2}{3}(-x-1) + \frac{4}{9} \right) \\
& \quad + \llbracket x < 0 \rrbracket \cdot \left(\frac{1}{2} \cdot \left(\frac{1}{3}(-x+1) + \frac{5}{9} \right) \right) \\
& = \llbracket x > 0 \rrbracket \cdot \left(\frac{1}{3}x + \frac{5}{9} \right) + \llbracket x < 0 \rrbracket \cdot \left(-\frac{2}{3}x + \frac{4}{9} \right) \\
& = G_{-x} \leq G_{+x}
\end{aligned}$$

We have by now established integrability of both ^+x and ^-x . Furthermore, we know that G_{+x} is an upper bound of the expected value of ^+x .

Alternatively, instead of proving integrability of ^+x and ^-x individually, we could have proved the integrability of $|x|$ using the simpler invariant G from the analysis using integrability witnessing pairs, see Appendix B1. We would then still need to find an upper bound for ^+x using invariant G_{+x} , but we would get rid of one of the complicated invariant, namely G_{-x} .

We now need to establish a lower bound for ^-x . For that, we need a lower ω -invariant H_n . Again, the simplest we were able to come up with is given by

$$H_n = \sum_{i=0}^n -\frac{\min \{(-1)^i \cdot (x + \text{sign}(x) \cdot i), 0\}}{2^{i+1}}.$$

For verifying that H_n is indeed an ω -invariant, we need to check two conditions. First, $^{1/2}_{C'}F_{-x}(\mathbf{0}) \geq H_0$:

$$\begin{aligned}
^{1/2}_{C'}F_{-x}(\mathbf{0}) &= \frac{1}{2} \cdot ^-x + \frac{1}{2} \cdot \text{wp}[C'](\mathbf{0}) \\
&= \frac{1}{2} \cdot ^-x + \frac{1}{2} \cdot \mathbf{0} \\
&= \frac{^-x}{2} \\
&= -\frac{\min\{x, 0\}}{2} \\
&= -\frac{\min \{(-1)^0 \cdot (x + \text{sign}(x) \cdot 0), 0\}}{2^{0+1}} \\
&= \sum_{i=0}^0 -\frac{\min \{(-1)^i \cdot (x + \text{sign}(x) \cdot i), 0\}}{2^{i+1}} \\
&= H_0 \geq H_0
\end{aligned}$$

Second, $^{1/2}_{C'}F_{-x}(H_n) \geq H_{n+1}$:

$$\begin{aligned}
^{1/2}_{C'}F_{-x}(H_n) &= \frac{1}{2} \cdot ^-x \\
&\quad + \frac{1}{2} \cdot \text{wp}[C'] \left(\sum_{i=0}^n -\frac{\min \{(-1)^i \cdot (x + \text{sign}(x) \cdot i), 0\}}{2^{i+1}} \right) \\
&= -\frac{\min\{x, 0\}}{2} + \frac{1}{2} \sum_{i=0}^n -\frac{N}{2^{i+1}},
\end{aligned}$$

where $N = \min \{(-1)^i \cdot (-x - \text{sign}(x))\}$

$$\begin{aligned}
& + \text{sign}(-x - \text{sign}(x)) \cdot i, 0\} \\
& = -\frac{\min \{(-1)^0 \cdot (x + \text{sign}(x) \cdot 0), 0\}}{2^{0+1}} \\
& \quad + \frac{1}{2} \sum_{i=0}^n -\frac{\min \{(-1)^i \cdot (-x + \text{sign}(x)) - \text{sign}(x) \cdot i, 0\}}{2^{i+1}} \\
& = -\frac{\min \{(-1)^0 \cdot (x + \text{sign}(x) \cdot 0), 0\}}{2^{0+1}} \\
& \quad + \sum_{i=0}^n -\frac{\min \{(-1)^{i+1} \cdot (x + \text{sign}(x) \cdot (i+1)), 0\}}{2^{i+1+1}} \\
& = -\frac{\min \{(-1)^0 \cdot (x + \text{sign}(x) \cdot 0), 0\}}{2^{0+1}} \\
& \quad + \sum_{i=1}^{n+1} -\frac{\min \{(-1)^i \cdot (x + \text{sign}(x) \cdot i), 0\}}{2^{i+1}} \\
& = \sum_{i=0}^{n+1} -\frac{\min \{(-1)^i \cdot (x + \text{sign}(x) \cdot i), 0\}}{2^{i+1}} \\
& = H_{n+1} \geq H_{n+1}
\end{aligned}$$

We can now argue that an upper bound for the expected value of x is given by

$$G_{+x} - \sup_{n \in \mathbb{N}} H_n.$$

Arguing about $\sup_{n \in \mathbb{N}} H_n$ is more involved than it was in the case of the integrability-witnessing expectation analysis where obtaining the supremum was immediate:

$$\begin{aligned}
\sup_{n \in \mathbb{N}} H_n &= \sup_{n \in \mathbb{N}} \sum_{i=0}^n -\frac{\min \{(-1)^i \cdot (x + \text{sign}(x) \cdot i), 0\}}{2^{i+1}} \\
&= \sum_{i=0}^{\omega} -\frac{\min \{(-1)^i \cdot (x + \text{sign}(x) \cdot i), 0\}}{2^{i+1}} \\
&= \sum_{i=0}^{\omega} -\frac{\min \{x + \text{sign}(x) \cdot 2i, 0\}}{2^{2i+1}} \\
&\quad + \sum_{i=0}^{\omega} -\frac{\min \{-x - \text{sign}(x) \cdot (2i+1), 0\}}{2^{2i+2}} \\
&= \llbracket x > 0 \rrbracket \left(\sum_{i=0}^{\omega} -\frac{\min \{x + \text{sign}(x) \cdot 2i, 0\}}{2^{2i+1}} \right. \\
&\quad \left. + \sum_{i=0}^{\omega} -\frac{\min \{-x - \text{sign}(x) \cdot (2i+1), 0\}}{2^{2i+2}} \right) \\
&\quad + \llbracket x < 0 \rrbracket \left(\sum_{i=0}^{\omega} -\frac{\min \{x + \text{sign}(x) \cdot 2i, 0\}}{2^{2i+1}} \right. \\
&\quad \left. + \sum_{i=0}^{\omega} -\frac{\min \{-x - \text{sign}(x) \cdot (2i+1), 0\}}{2^{2i+2}} \right) \\
&= \llbracket x > 0 \rrbracket \left(\sum_{i=0}^{\omega} -\frac{0}{2^{2i+1}} + \sum_{i=0}^{\omega} -\frac{-x - (2i+1)}{2^{2i+2}} \right)
\end{aligned}$$

$$\begin{aligned}
& + \llbracket x < 0 \rrbracket \left(\sum_{i=0}^{\omega} -\frac{x-2i}{2^{2i+1}} + \sum_{i=0}^{\omega} -\frac{0}{2^{2i+2}} \right) \\
& = \llbracket x > 0 \rrbracket \left(\sum_{i=0}^{\omega} \frac{x+2i+1}{2^{2i+2}} \right) + \llbracket x < 0 \rrbracket \left(\sum_{i=0}^{\omega} \frac{-x+2i}{2^{2i+1}} \right) \\
& = \llbracket x > 0 \rrbracket \cdot \left(\frac{1}{3}x + \frac{5}{9} \right) + \llbracket x < 0 \rrbracket \cdot \left(-\frac{2}{3}x + \frac{4}{9} \right) \\
& \quad \text{(obtained with the aid of Wolfram|Alpha)} \\
& = G_{-x}
\end{aligned}$$

Finally, we can calculate an upper bound for the expected value of x by

$$\begin{aligned}
& G_{+x} - \sup_{n \in \mathbb{N}} H_n \\
& = G_{+x} - G_{-x} \\
& = \llbracket x > 0 \rrbracket \cdot \left(\frac{2}{3}x + \frac{4}{9} \right) + \llbracket x < 0 \rrbracket \cdot \left(-\frac{1}{3}x + \frac{5}{9} \right) \\
& \quad - \left(\llbracket x > 0 \rrbracket \cdot \left(\frac{1}{3}x + \frac{5}{9} \right) + \llbracket x < 0 \rrbracket \cdot \left(-\frac{2}{3}x + \frac{4}{9} \right) \right) \\
& = \llbracket x > 0 \rrbracket \cdot \left(\frac{2}{3}x + \frac{4}{9} - \frac{1}{3}x - \frac{5}{9} \right) \\
& \quad + \llbracket x < 0 \rrbracket \cdot \left(-\frac{1}{3}x + \frac{5}{9} + \frac{2}{3}x - \frac{4}{9} \right) \\
& = \llbracket x > 0 \rrbracket \cdot \left(\frac{x}{3} - \frac{1}{9} \right) + \llbracket x < 0 \rrbracket \cdot \left(\frac{x}{3} + \frac{1}{9} \right) \\
& = \frac{x}{3} + \frac{\llbracket x > 0 \rrbracket \cdot (-1) + \llbracket x < 0 \rrbracket \cdot 1}{9} \\
& = \frac{x}{3} - \frac{\text{sign}(x)}{9}
\end{aligned}$$

and we obtain the same result as we did with the integrability–witnessing expectation analysis.

C. Loop Invariants for Lower Bounds

If we take a closer look at the sequence

$$\left(\bigwedge_{C'F_{|f|+f}^n(\mathbf{0}) - C'F_{|f|}^n(\mathbf{0}), C'F_g^n(\mathbf{0}) \right)_{n \in \mathbb{N}}$$

we can see that in order to under-approximate the limit of that sequence, we can—simply put—

- 1) over-approximate the limit—i.e. the supremum—of $C'F_g^n(\mathbf{0})$,
- 2) under-approximate the limit—i.e. again the supremum—of $C'F_{|f|+f}^n(\mathbf{0})$, and
- 3) over-approximate the limit—once again: the supremum—of $C'F_{|f|}^n(\mathbf{0})$.

Notice that these over- and under-approximations are over- and under-approximations of standard weakest pre-expectations. Furthermore, recall that by Theorem 1 (4) and (5) we have invariant rules for those over- and under-approximations. This immediately leads us to the following proof rule for loops:

Theorem 7 (Loop Invariants for Lower Bounds of $\widetilde{\text{wp}}$). *Let $\langle f, g \rangle \in \mathbb{IE}$, $C' \in \text{pProgs}$, $I, G \in \mathbb{E}_{\geq 0}^\infty$ with $G(\sigma) < \infty$,*

for all $\sigma \in \Sigma$, and $(H_n)_{n \in \mathbb{N}} \subseteq \mathbb{E}_{\geq 0}^\infty$. Then $C'F_g(G) \leq G$, $C'F_{|f|}(I) \leq I$, $H_0 \leq C'F_{|f|+f}(\mathbf{0})$, and $H_{n+1} \leq C'F_{|f|+f}(H_n)$ implies

$$\left(\sup_{n \in \mathbb{N}} H_n - I, 2 \cdot G \right) \sqsubseteq \widetilde{\text{wp}}[\text{while}(\xi)\{C'\}]\langle f, g \rangle.$$